



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

ITW -

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,548	02/25/2002	Curtis E. Stevens	01-1008	7976

7590 09/23/2005

LOREN H. McROSS  
PHOENIX TECHNOLOGIES LTD.  
411 EAST PLUMERIA DRIVE  
SAN JOSE, CA 95134

RECEIVED  
OIPR/MA

SEP 30 2005

EXAMINER	
GEBRESILASSIE, KIBROM K	
ART UNIT	PAPER NUMBER
2128	

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/084,548	STEVENS, CURTIS E.
	<b>Examiner</b>	<b>Art Unit</b>
	Kibrom K. Gebresilassie	2128

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 25 February 2002.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-6 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-6 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 25 February 2002 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|  | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

1. This action is responsive to the application filed on February 25, 2002.
2. Claims 1-6 have been examined and rejected.

#### ***Oath/Declaration***

3. The Office acknowledges receipt of a properly signed oath/declaration filed on February 2, 2002.

#### ***Specification***

4. The disclosure is objected to because of the following informalities: Page 4 line 8, "hard disk drive 20" should be read as "hard disk drive 30".

Appropriate correction is required.

#### ***Drawings***

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: **Fig. 1, blocks 18, 19, 21, 22, and 23.** Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

6. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "11" and "22" have both been used to designate CPU and reference characters "13" and "23" have both also been used to designate MEMORY. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-6 are rejected under 35 U.S.C. 102(b) as being anticipated by "Information Technology –Protected Area Run Time Interface Extension Services" printed September 30, 2000 by American National Standards, Inc.

**As per Claim 1:**

Stevens discloses a method for use with a computer system having an operating system (page 4 "3.2.17 O/S") and a nonvolatile storage device (hard disk; page 1 under a title of "1 Scope" line 2), comprising the steps of:

creating a boot engineering extension record (BEER) on the nonvolatile storage device (page 7 under a title of "5.2 The Boot Engineering Extension Record (BEER)");  
configuring the boot engineering extension record to have SETMAX pointer that points to a user area of the nonvolatile storage device and a service area pointer (page 6 under a title "4 Overview" lines 1-2) that points to a PARTIES service area that is part of a host protected area of the nonvolatile storage device (page 6 under a title of "5 Initialization Requirements" lines 1-5);

storing data derived from the removable storage media device in the PARTIES service area, which data will be used in an emulated removable storage media device (page 5 under a title of " 3.2.24" lines 1-2); and

configuring an operating system to access the PARTIES service area so that the data stored therein is presented to a user as if it were derived from an emulated removable storage media device (page 6 under a title "4 Overview" lines 10-15).

**As per Claim 2:**

The method recited in claim 1 further comprising the step of: configuring the operating system to access the user area (page 5 "3.2.25 User Area" to provide access to applications and data of a user of the computer system (page 9 under a title of "5.2.3.4 Bit 4" lines 5-6).

**As per Claim 3:**

The limitation of claim 3 has already been discussed in the rejection of claim 1. It is therefore rejected under the same rationale.

**As per Claim 4:**

The limitation of claim 4 has already been discussed in the rejection of claim 2. It is therefore rejected under the same rationale.

**As per Claim 5:**

A computer system comprising  
a central processing unit (x86 processor; page 1 under a title of "1 Scope" line 22) ;  
a system memory (system memory; page 5 under a title "3.2.19 Protect Mode line 3);  
a nonvolatile storage device (hard disk; page 1 under a title of "1 Scope" line 2);  
an operating system (page 4 under a title of "3.2.17 O/S"); and  
computer software (page 9 under a title of "5.2.3.4 Bit (Configuration Time Stamp is  
Valid)" lines 1-3) that creates a boot engineering extension record (BEER) on the nonvolatile  
storage device(page 7 under a title "5.2 The Boot Engineering Extension Record (BEER)'),  
configures the boot engineering extension record to have SETMAX pointer that points to a user  
area of the hard disk drive and a service area pointer (page 6 under a title "4 Overview" lines 1-  
2) that points to a PARTIES service area that is part of a host protected area of the nonvolatile  
storage device, stores data derived from the removable storage media device in the PARTIES  
service area, which data will be used in an emulated removable storage media device, and  
configures an operating system to access the PARTIES service area so that it is presented to a  
user as being derived from an emulated removable storage media device(page 6 under a title "4  
Overview" lines 10-15).

**As per Claim 6:**

The limitation of claim 6 has already been discussed in the rejection of claim 2. It is  
therefore rejected under the same rationale.

***Conclusion***

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
2. Any inquiring concerning this communication or earlier communication from the examiner should be directed to Kibrom K. Gebresilassie whose telephone number is (571) 272-

Art Unit: 2128

8571. The examiner can normally be reached on Monday-Friday, 8:30 am to 4:30 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner supervisor, Jean R. Homere can be reached at (571) 272-3780. The official fax number is (703) 872-9306. Any inquiring of a general nature relating to the status of this application should be directed to the group receptionist whose telephone number is (571) 272-3700.

**Kibrom K. Gebresilassie**  
Patent Examiner  
U.S. Patent and Trademark Office  
Simulation and Emulation, Art Unit 2128  
401 Dulany St., Room 5C25 (Randolph)  
Alexandria, VA 22314-5774  
Tel: 571-272-8571  
[Kibrom.gebresilassie@uspto.gov](mailto:Kibrom.gebresilassie@uspto.gov)



A handwritten signature in black ink, appearing to read "Kibrom K. Gebresilassie". The signature is fluid and cursive, with "Kibrom" on top and "K. Gebresilassie" below it.

<b>Notice of References Cited</b>		Application/Control No.	Applicant(s)/Patent Under Reexamination STEVENS, CURTIS E.	
		Examiner Kibrom K. Gebresilassie	Art Unit 2128	Page 1 of 1

**U.S. PATENT DOCUMENTS**

* 	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
A	US-2002/0133702 A1	09-2002	Stevens, Curtis E.	713/163
B	US-6,633,976 B1	10-2003	Stevens, Curtis E.	713/2
C	US-2004/0243759 A1	12-2004	Itoh et al.	711/112
D	US-2003/0079101 A1	04-2003	Oh, Sang-Min	711/173
E	US-6,772,313	08-2004	Oh, Sang-Min	711/173
F	US-			
G	US-			
H	US-			
I	US-			
J	US-			
K	US-			
L	US-			
M	US-			

**FOREIGN PATENT DOCUMENTS**

* 	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
N					
O					
P					
Q					
R					
S					
T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
U		Curtis E. Stevens, Information Technology -Protected Area Run Time Interface Services,September 30, 2000,American National Standards Institute,1-19.
V		Narayan Khalsa,ImageCast MFG/Area51/PXE Inegration,2001,StorageSoft, Inc.
W		Jason Hayes,Area51 Onboard System Recovery,2000,StorageSoft,Inc.
X		

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

**Revision 3  
September 30, 2000**

---

## **Information Technology - Protected Area Run Time Interface Extension Services**

This is an internal working document of T13, a Technical Committee of Accredited Standards Committee NCITS. As such, this is not a completed standard and has not been approved. The T13 Technical Committee may modify the contents. The contents are actively being modified by T13. This document is made available for review and comment only.

Permission is granted to members of NCITS, its technical committees, and their associated task groups to reproduce this document for the purposes of NCITS standardization activities without further permission, provided this notice is included. All other rights are reserved. Any commercial or for-profit replication or republication is prohibited.

T13 Technical Editor:

Curtis E. Stevens  
Phoenix Technologies LTD  
135 Technology Drive  
Irvine, Ca. 92618  
USA

Tel: (949) 790-2121  
Fax: (949) 790-2003  
Email: [Curtis\\_Stevens@Phoenix.com](mailto:Curtis_Stevens@Phoenix.com)



Other Points of Contact:

**T13 Chair**  
**Gene Milligan**  
**Seagate Technology**  
**OKM 251**  
**10323 West Reno (West Dock)**  
**P.O. Box 12313**  
**Oklahoma City, OK 73157-2313**  
Tel: 405-324-3070  
Fax: 405-324-3794

**T13 Vice-Chair**  
**Pete McLean**  
**Maxtor Corporation**  
**2190 Miller Drive**  
**Longmont, CO 80501**  
Tel: 303-678-2149  
Fax: 303-682-4811

**NCITS Secretariat**  
**Administrator Standards Processing**  
**1250 Eye Street, NW Suite 200**  
**Washington, DC 20005**  
Tel: 202-737-8888  
Fax: 202-638-4922  
Email: NCITS@ITIC.NW.DC.US

**T13 Reflector**

Internet address for subscription to the T13 reflector: majordomo@dt.wdc.com  
Send email to above account and include in BODY of text, on a line by itself the following:  
"subscribe T13 [your email address]"  
Internet address for distribution via T13 reflector: T13@dt.wdc.com

**T13 WEB site**  
[www.t13.org](http://www.t13.org)

**T13 mailings**  
**Global Engineering**  
**15 Inverness Way East**  
**Englewood, CO 80112-5704**  
Tel: 303-792-2181 or 800-854-7179  
Fax: 303-792-2192

**T13/1367D Revision 3**

**DOCUMENT STATUS**

**Revision 0 - August 23, 1999**

Initial revision, document created from D98131r2.

**Revision 1 - February 18, 2000**

Incorporates changes from meetings held after 23-AUG-99

**Revision 2 - April 5, 2000**

Incorporates changes from meetings held after 18-FEB-00

**Revision 3 - September 30, 2000**

Incorporates changes from E00133r1 (resolution of letter ballot comments)

ANSI®  
NCITS.\*\*\*\*-200x

American National Standard  
for Information Systems -

## Protected Area Run Time Interface Extension Services

Secretariat  
**Information Technology Industry Council**

Approved mm dd yy

**American National Standards Institute, Inc.**

### **Abstract**

This standard specifies a firmware (BIOS) interface for addressing an area of ATA devices that is normally hidden via the SET MAX ADDRESS command. This firmware interface builds on ATA/ATAPI-4 (NCITS 317-1998) to provide services that an operating system may use to address the hidden area in the same manner as a removable media device.

## American National Standard

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer. Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give interpretation on any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

**CAUTION NOTICE:** This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

**CAUTION:** The developers of this standard have requested that holder's of patents that may be required for the implementation of the standard, disclose such patents to the publisher. However, neither the developers nor the publisher have undertaken a patent search in order to identify which, if any, patents may apply to this standard.

As of the date of publication of this standard and following calls for the identification of patents that may be required for the implementation of the standard, no such claims have been made.

The developer or the publisher in respect to any standard it processes conducts no further patent search. No representation is made or implied that licenses are not required to avoid infringement in the use of this standard. See clause 2.

Published by

**American National Standards Institute**

**11 West 42nd Street, New York, New York 10036**

Copyright 200n by American National Standards Institute

All rights reserved.

<b>Contents</b>	<b>Page</b>
Foreword.....	ii
Introduction.....	v
1 Scope .....	1
2 Normative References .....	1
2.1 Approved references.....	2
2.2 References under development.....	2
2.3 Other references .....	2
3 Keyword, definitions, abbreviations, and conventions .....	2
3.1 Keywords .....	2
3.2 Definitions and Abbreviations.....	3
4 Overview.....	6
5 Initialization Requirements.....	6
5.1 Diagnostic Service (DS) .....	6
5.2 The Boot Engineering Extension Record (BEER) .....	7
5.3 BEER Directory of Services Description.....	11
6 Runtime Services.....	13
6.1 INT 13h Dispatcher.....	13
6.2 Reset.....	13
6.3 Get Status .....	14
6.4 Read Sectors.....	14
6.5 Write Sectors .....	15
6.6 Verify Sectors .....	15
6.7 Format Track.....	16
6.8 Get Device Parameters.....	16
6.9 Get Current Device Parameters.....	16
6.10 Get Device Change Status .....	17
6.11 Set Device Type.....	17
6.12 Set Media Type for Format .....	17
6.13 Sense Media Type .....	18
6.14 Check Extensions Present .....	18
6.15 Get Device Parameters.....	18

<b>Table</b>	<b>Page</b>
1 Boot Engineer Extension Record.....	8
2 BEER Directory of Services Entry.....	11
3 Result Buffer .....	19

## Foreword

(This foreword is not part of American National Standard NCITS.xxx-200x)

Hard disk drives have been returned to system manufacturers in unacceptably large numbers. Analysis of the returned drives by these system manufacturers reveals that the vast majority of returned disk drives are fully functional. Further, a significant percentage of the returned merchandise that did have defects were damaged in shipping. PC Computer System manufacturers are attempting to better support their products by placing information that is normally shipping on an external floppy, CD, or DVD directly on the primary storage device. The vast majority of laptop and desktop computers use ATA hard drives as the primary storage device. This standard defines a method and supporting services for placing data and/or programs on the hard drive in an area that is normally not available to the user.

Requests for interpretation, suggestions for improvement and addenda, or defect reports are welcome. They should be sent to the NCITS Secretariat, Information Technology Industry Council, 1250 I Street NW, Suite 200, Washington, DC 20005-3922.

This standard was processed and approved for submittal to ANSI by National Committee for Information Technology Standardization (NCITS). Committee approval of this standard does not necessarily imply that all committee members voted for approval. At the time it approved this standard, NCITS had the following members:

Karen Higginbottom, Chair

(Vacant), Vice-Chair

Monica Vago, Secretary

Organization Represented.....	Name of Representative
AMP, Inc .....	John Hill
	Charles Brill (Alt.)
Apple Computer .....	David Michael
	Jerry Kellenbenz (Alt.)
AT&T.....	Thomas Frost
	Paul Bartoli (Alt.)
Bull HN Information Systems, Inc.....	Patrick L. Harris
Compaq Computer Corporation .....	Steven Heil
	Seve Park (Alt.)
Eastman Kodak.....	Michael Nier
Hewlett-Packard.....	Karen Higginbottom
	Donald Loughry (Alt.)
Hitachi America, Ltd. ....	John Neumann
	Kei Yamashita (Alt.)
Hughes Aircraft Company.....	Harold L. Zebrack
IBM Corporation.....	Ron Silletti
	Joel Urman (Alt.)
Institute for Certification of Computer Professionals .....	Kenneth M. Zemrowski
	Tom Kurihara (Alt.)
Lucent Technologies, Inc.....	Herbert Bertine
	Tom Rutt (Alt.)
National Communications Systems .....	Dennis Bodson
	Frack McClelland (Alt.)
National Institute of Standards and Technology .....	Michael Hogan
	Bruce K. Rosen (Alt.)
Panasonic Technologies, Inc.. .....	Judson Hofmann
	Terry J. Nelson (Alt.)
Share, Inc.....	David Thewlis

Gary Ainsworth (Alt.)

Masataka Ogawa

Michael Deese (Alt.)

Sony Electronics, Inc. ....

**T13/1367D Revision 3**

Organization Represented.....	Name of Representative
Storage Technology Corporation .....	Joseph S. Zajaczkowski
Sun Microsystems, Inc. ....	Gary Robinson
Sybase, Inc. ....	Donald Deutsch Andrew Eisenberg (Alt.)
Texas Instruments, Inc.....	Clyde Camp Fritz Whittington (Alt.)
Unisys Corporation.....	Arnold F. Winkler Stephen P. Oksala (Alt.)
U.S. Department of Defense/DISA.....	Jerry L. Smith C. J. Pasquariello (Alt.)
U.S. Department of Energy .....	Carol Blackston Bruce R. White (Alt)
Xerox Corporation .....	John B. Flannery Jean Baroness (Alt.)

Subcommittee T13 on ATA Interfaces, that reviewed this standard, had the following members:

Gene Milligan, Chairman

Pete McLean, Vice-Chairman

Kent Pryor, Secretary

Amy Barton	Gene Milligan	Richard Harcourt [Alternate]
Darrin Bulik	Masataka Ogawa	LeRoy Leach [Alternate]
Litko Chan	Darrell Redford	Wen Lin [Alternate]
Ben Chang	Ron Roberts	James McGrath [Alternate]
Dan Colegrove	Matt Rooke	Kha Nguyen [Alternate]
Tom Colligan	Bob Salem	Marc Noblitt [Alternate]
David Dickson	Curtis Stevens	Yogi Schaffner [Alternate]
Greg Elkins	Tim Thompson	Paresh Sheth [Alternate]
Mark Evans	Anthony Yang	Ron Stephens [Alternate]
Tony Goodfellow	Ken Bovatsek [Alternate]	Seiro Taniyama [Alternate]
Tasuku Kasebayashi	Tim Bradshaw [Alternate]	Tokuyuki Totani [Alternate]
Hale Landis	Andy Chen [Alternate]	Tri Van [Alternate]
Ming Louie	Renee Depew [Alternate]	Quang Vuong [Alternate]
Pete McLean	Tom Hanan [Alternate]	Sam Wong [Alternate]

ATA/ATAPI ad hoc Working Group, that developed this standard, had the following additional participants:

Charles Brill	Jonathan Hanmann	Lawrence Lamers
Mike Christensen	Jim Hatfield	Raymond Liu
Michael Eschmann	Richard Kalish	Kent Pryor
Jon Haines	Eric Kvamme	Paul Raikonen

## Introduction

This standard encompasses the following:

Clause 1 describes the scope.

Clause 2 provides normative references used within this document.

Clause 3 provides definitions, abbreviations, and conventions used within this document.

Clause 4 describes the overview of the document content.

Clause 5 describes the system initialization requirements.

Clause 6 describes the runtime services

This Page Blank (uspto)

## American National Standard for Information Systems -

# Information Technology - Protected Area Run Time Interface Extension Services – PARTIES

## 1 Scope

This standard describes a BIOS firmware layer that may be used to both place and execute system diagnostics on a protected area of the system hard disk. The purpose of these diagnostics is to accurately determine for both the user and a technical support engineer that the hard drive is functioning correctly. These diagnostics are placed in a protected area of the disk drive because they are less vulnerable to attack from viruses, system software corruption, and the user. The firmware layer described herein may also be used to run DOS based rescue utilities once the drive has been shown to be working by the diagnostics described above. The net effect of these capabilities is that a system may ship with embedded diagnostic and rescue capabilities, these capabilities are known to be reliable by the system manufacturer, and may not be easily corrupted by the user.

The BIOS firmware described in this standard may be implemented for any disk drive that conforms to NCITS 317-1998 (ATA/ATAPI-4) and implements the SET MAX command. The SET MAX command as it is defined in NCITS 317-1998 provides a great deal of security for hiding data on the disk drive. If the system is unable to boot the primary operating system, the area protected by the SET MAX ADDRESS command remains bootable.

All the fields described in this standard are designed to last at least 20 years, given a doubling in capacity each year.

This standard describes a method for the BIOS to do the following:

- Find the start of the reserved area boot code and issue SET MAX ADDRESS command,
- Emulate the reserved area boot code as a bootable floppy.

This standard employs a method that is flexible enough to allow the reserved area boot code to be seen as the primary floppy drive.

Note - This standard only describes BIOS implementations using x86 processor architectures. Some operating systems and applications employ proprietary methods to access floppy and hard drives. The BIOS firmware layer described in this document does not address software that addresses the media in a proprietary manner.

## 2 Normative References

The following standards contain provisions that, through reference in the text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

Copies of the following documents can be obtained from ANSI: Approved ANSI standards, approved and draft international and regional standards (ISO, IEC, CEN/CENELEC, ITUT), and approved and draft foreign standards (including BSI, JIS, and DIN). For further information, contact ANSI Customer Service Department at 212-642-4900 (phone), 212-302-1286 (fax) or via the World Wide Web at <http://www.ansi.org>.

Additional availability contact information is provided below as needed.

## **2.1 Approved references**

The following approved ANSI standards and technical reports, approved international and regional standards and technical reports (ISO, IEC, CEN/CENELEC, ITUT), may be obtained from the international and regional organizations who control them.

ATA/ATAPI-4 NCITS 317-1998

BIOS Enhanced Disk Drive Technical Report NCITS TR-21

## **2.2 References under development**

At the time of publication, the following referenced standards were still under development. For information on the current status of the document, or regarding availability, contact the relevant standards body or other organization as indicated.

ATA/ATAPI-5 NCITS 1321D

BIOS Enhanced Disk Drive Services (EDD) NCITS 1386D

For more information on the current status of the above documents, contact NCITS. To obtain copies of these documents, contact Global Engineering or NCITS.

## **2.3 Other references**

The following standard and specifications were also referenced.

BIOS Boot Specification (Compaq, Phoenix and Intel), [www.phoenix.com/techs/specs.html](http://www.phoenix.com/techs/specs.html)

# **3 Keyword, definitions, abbreviations, and conventions**

## **3.1 Keywords**

Several keywords are used to differentiate between different levels of requirements and optionality.

### **3.1.1 Mandatory**

A keyword indicating items to be implemented as defined by this standard.

### **3.1.2 May**

A keyword that indicates flexibility of choice with no implied preference.

### **3.1.3 Optional**

A keyword that describes features that are not required by this standard. However, if any optional feature defined by the standard is implemented, it shall be done in the way defined by the standard. Describing a feature as optional in the text is done to assist the reader.

### **3.1.4 Reserved**

A keyword indicating reserved bits, bytes, words, fields, and code values that are set aside for future standardization. Their use and interpretation may be specified by future extensions to this or other standards. A reserved bit, byte, word, or field shall be set to zero, or in accordance with a future extension to this standard. The recipient shall not check reserved bits, bytes, words, or fields. Receipt of reserved code values in defined fields shall be treated as an error.

### **3.1.5 Shall**

A keyword indicating a mandatory requirement. Designers are required to implement all such mandatory requirements to ensure interoperability with other standard conformant products.

### **3.1.6 Should**

A keyword indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase "it is recommended".

## **3.2 Definitions and Abbreviations**

For the purposes of this standard, the following definitions apply:

### **3.2.1 ATA**

An AT Attachment device, also known as an IDE device, is a hard drive that conforms to an ATA standard.

### **3.2.2 BDA**

The BIOS Data Area is an area of reserved memory used by the BIOS and O/S to store data about the system hardware. It is located at memory segment 40h starting with 40h:00h.

### **3.2.3 BIOS**

The Basic Input/Output System is the firmware embedded on a chip located on the computer's main board. The BIOS executes POST to test and initialize the system components and then loads the O/S. The BIOS also handles the low-level Input/Output to the various peripheral devices connected to the computer.

### **3.2.4 Boot Device**

A Boot Device is any device that shall be initialized prior to loading the O/S. This includes the primary input device (keyboard), the primary output device (display), and the initial program load device (floppy drive, hard drive, etc.)

### **3.2.5 Byte**

A byte is a unit of data that consists of eight bits as described below:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
-------	-------	-------	-------	-------	-------	-------	-------

### **3.2.6 CHS**

CHS addressing: CHS addressing is a method of addressing the contents of a storage device using logical cylinders (C), logical heads (S), and logical sectors (S). This method of addressing allows a maximum C=16383, H=16, S=63, or 8.4GB. See LBA for another addressing method.

### **3.2.7 DOS**

DOS is a Disk Operating System that uses the system BIOS as a firmware abstraction layer to access system hardware. Examples of DOS operating systems include MS-DOS®, DR-DOS®, PC-DOS®, Free DOS, Windows® 3.11, and Windows® 95.

### 3.2.8 DWord

A DWord (Double Word) is a unit of data that consist of four bytes. This data is usually represented on paper as a series of bits numbered from 31 to 0. Byte 0 of a Dword is stored in the lowest byte address and Byte 3 is stored in the highest byte address.

**On Paper:**

Bit 31	Byte 3	Byte 2	Byte 1	Byte 0	Bit 0
--------	--------	--------	--------	--------	-------

**In Memory:**

Bit 7	Bit 0	Byte 0	Byte 1	Byte 2	Byte 3	Bit 31	Bit 24
-------	-------	--------	--------	--------	--------	--------	--------

### 3.2.9 Host

The Host is the computer system that is controlled by the BIOS.

### 3.2.10 Host Protected Area

The area of the disk drive's storage capacity not normally accessible by the user. It starts at the max address + 1 and goes to the address returned by READ NATIVE MAX ADDRESS.

### 3.2.11 INT 13h

A BIOS interrupt service which provides a protocol independent method for accessing floppy and hard drives.

### 3.2.12 INT 40h

A BIOS interrupt service which provides a protocol independent method for accessing INT 13h devices that have a device number less than or equal to 7Fh.

### 3.2.13 IPL Device

An Initial Program Load Device is any device in the system that may boot and load an O/S. In standard AT machines, this is the floppy drive or hard drive.

### 3.2.14 LBA

LBA is a method of addressing a device, which involves using a Logical Block Address. This method of addressing allows a maximum address of  $2^{28}-1$ , or 137.4GB of data. See CHS for another address method.

### 3.2.15 Max address

The Max address is the last LBA accessible to the end user on the hard disk.

### 3.2.16 NV Memory

Non-Volatile memory is memory that retains its content even when the power has been shut off. The most common type of NV memory on a PC is the CMOS RAM that is used to store system configuration information.

### 3.2.17 O/S

An operating system is the initial program that is loaded from an IPL device when that device is selected for booting.

### 3.2.18 POST

The Power-On Self-Test is the part of the BIOS that takes control immediately after the computer is turned on. POST initializes the computer hardware so that an O/S may be loaded.

### 3.2.19 Protect Mode

Intel x86 processors have several modes of main memory addressing. One of these modes is called Real Mode. In this mode, systems can only address the first mega-byte of memory. Another mode is Protect Mode. In this mode all the system memory can be addressed.

### 3.2.20 Qword

A QWord (Quad Word) is a unit of data that consist of eightbytes. This data is usually represented on paper as a series of bits numbered from 63 to 0. Byte 0 of a Qword is stored in the lowest byte address and Byte 7 is stored in the highest byte address.

#### On Paper:

Bit 63	Byte 7	Byte 6	Byte 5	Byte 4	Byte 3	Byte 2	Byte 1	Byte 0	Bit 0
--------	--------	--------	--------	--------	--------	--------	--------	--------	-------

#### In Memory:

Bit 7	Bit 0	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Bit 63	Bit 57
-------	-------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------

### 3.2.21 Service Area

An area of the Host Protected Area reserved for a particular BIOS service.

### 3.2.22 Standard Floppy Drive

The Standard Floppy Drive is the generic term to define the currently used 5.25" floppy drives and the 3.5" floppy drives found in most systems shipping today.

### 3.2.23 System Vendor

Vendor who has access to the Host Protected Area and may create and add code to Service Areas.

### 3.2.24 Trusted Code

Code that resides in the Host Protected Area that is trusted to operate without corruption of the structure or data in the User or Host Protected Areas.

### 3.2.25 User Area

The area of the hard disk drive that is available to all users. This area is defined from LBA zero to the max address.

### 3.2.26 Warm Boot

A Warm Boot is a system re-boot where the system hardware reset is not asserted. A host may initiate a software reset on a device by setting SRST in the Device Control register to one (see ATA/ATAPI-5).

### 3.2.27 Word

A word is a unit of data that consist of two bytes. This data is usually represented on paper as a series of bits numbered from 15 to 0. Byte 0 of a Word is stored in the lower byte address and Byte 1 is stored in the higher byte address.

#### On Paper:

																Byte 1	Byte 0														
																15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

#### In Memory:

								Byte 1								Byte 0	Byte 1														
																7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8

## 4 Overview

The SET MAX ADDRESS command allows the hard drive's storage capacity to be divided into two areas, the User Area and the Host Protected Area (includes the Boot Code Service Area). This standard describes a method for the BIOS to find the max address and then address the Boot Code Service Area as a floppy disk drive. The User Area extends from LBA zero to max address. The Host Protected Area extends from the max address + 1 to the last physical LBA of the device (native max address). The BIOS may use the Host Protected Area to provide a number of services; each service is allocated in its own region of the Host Protected Area. The allocation of these regions shall be under the control of the Boot Engineering Extension Record (BEER) Directory of Services structure. The system normally boots from the User Area. Booting from a Service Area may occur for diagnostic and recovery operations.

When the BIOS boots from a Service Area it puts the system into a Trusted Mode where the whole device is accessible to the Trusted Code (Trusted O/S) loaded by the BIOS. Once the BIOS has initiated the boot process on a Service Area, all accesses to the Service Area are accomplished through INT 13h device 00h (floppy drive emulation). This allows the User Area to remain at its original INT 13h device number, normally device 80h. Any devices that would normally have an ID's of 00h-7Fh shall have their device ID incremented by one.

Before the BIOS initiates a conventional boot, after the completion of the ROM scan and prior to the INT 19h call, it shall issue a SET MAX ADDRESS (non-volatile) command to the device to reset the max address.

## 5 Initialization Requirements

In order for the BIOS to determine the current Host Protected Area configuration, and the start of the Host Protected Area, a sector is allocated at the physical last sector of the hard disk to provide information about the Host Protected Area. This sector provides the geometry of the User Area, Start of Protected area and Start of reserved area boot code LBA among other things. The first 128 bytes of the sector are the Boot Engineering Extension Record (BEER). Following the BEER entry may be the optional BEER Directory of Services, which is a table with 64 byte entries. The Directory of Services immediately follows the BEER data and may contain up to six entries. The six entries at 64 bytes each plus the 128 BEER bytes compose the 512 bytes in the last sector on the device. IDENTIFY DEVICE data words 60 and 61 are modified by the SETMAX command to indicate the total number of user addressable sectors.

### 5.1 Diagnostic Service (DS)

One of the basic services to be made available is some form of diagnostic capability. Although there may be a number of diagnostic services available at most one shall be designated as the bootable Diagnostic Service. In some circumstances such as a faulty cable or host bus, accessing a failing device may reduce the chance of data recovery using special procedures. Thus before launching the bootable Diagnostic Service the system should perform the Built In Boot Device Integrity Check (BIBDIC). Once communication and basic device integrity has been established the Diagnostic Service may be launched either directly or indirectly as described below.

#### 5.1.1 Built In Boot Device Integrity Check

The Host BIOS shall have sufficient built in diagnostic code to determine that the basic I/O structure is working (i.e. PIO operation should be possible). The next step is to gain confidence that the storage device is working properly. This basic confidence test should be undertaken using SMART commands.

BIBDIC uses the SMART Short Self-Test in Captive Mode to test the device. It may not be possible to always detect if the fault is in the device, the cable, the Host adapter or the Host Bus system.

### **5.1.2 Recommended BIOS Menu Structure**

It is recommended that the BIOS not attempt to address and load the User BIOS Services until requested by user input. This gives the user a chance to choose the diagnostics option first and ensure that the disk system passes the BIBDIC before accessing the device

### **5.1.3 Recommended Check Sequence**

- If SMART capable
  - Issue the SMART ENABLE command
  - Issue the SMART RETURN STATUS command
  - If no response is received then the device, cable, or adapter is faulty and BIBDIC has failed.
  - If an error is received either SMART has been turned off or device has failed.
- Issue the IDENTIFY DEVICE command
  - If the returned information indicates that it is an ATA/ATAPI-5 device check the Checksum word.
  - If there is an error the transfer has failed and the subsystem is faulty, BIBDIC failed.
- If the device supports SMART and supports the SMART EXECUTE OFFLINE IMMEDIATE SHORT SELF-TEST IN CAPTIVE MODE then
  - Initiate the SMART EXECUTE OFFLINE IMMEDIATE SHORT SELF-TEST IN CAPTIVE MODE command. The device shall then instigate internal diagnostic procedures (it is recommended that the user be told to wait as this operation may take up to 2 minutes).
  - If the device fails these tests the BIBDIC has failed.
- If the IDENTIFY DEVICE data indicates that the device does not support the Host Protected Feature Set the BIBDIC has passed.
- If this is a warm boot issue the SET MAX UNLOCK Command (ATA/ATAPI-5 Devices) using the retained password.
- Store the device size data from the IDENTIFY DEVICE word.
- Issue the READ NATIVE MAX ADDRESS command to determine the actual maximum size of the device and compare with the IDENTIFY DEVICE data. This indicates if there is a Host Protected Area currently active, if there is use the SET MAX ADDRESS command (volatile) to the full size of the device.
- Read the last sector of the device, which should contain the BEER record. Validate the BEER record and then search its Directory of Services for the Diagnostic Service requested by the user, launch that service by booting directly or indirectly as indicated in the DS entry.
- The code in that Service Area may then perform more extensive diagnostics and/or recovery processes.

## **5.2 The Boot Engineering Extension Record (BEER)**

The purpose of this structure is to provide non-volatile configuration information about the device. The BEER is a data structure that is stored on the native maximum address of the device. The BEER consists of a mandatory header and one or more optional Directory of Service entries. The BIOS shall use the SET MAX ADDRESS command (non-volatile) to hide this record during the normal boot process. Table 1 shows the BEER header structure. The BEER record shall be accessed using an INT 13h call to the last sector of the device. In some instances the record returned may have been generated by the BIOS or ROM code and not read from surface of the device.

The remainder of this section describes the BEER header structure.

Table 1 - Boot Engineer Extension Record

Offset	Type	Description																				
0-1	Word	Signature = BEEFh																				
2-3	Word	BEER size. Shall be 128.																				
		<b>Capabilities Word</b>																				
		<table border="1"> <thead> <tr> <th>Bit</th><th>Description</th></tr> </thead> <tbody> <tr><td>8-15</td><td>Reserved</td></tr> <tr><td>7</td><td>Read Only</td></tr> <tr><td>6</td><td>Generated Record</td></tr> <tr><td>5</td><td>Use Reserved Area Boot Code Address</td></tr> <tr><td>4</td><td>Configuration Time Stamp is valid</td></tr> <tr><td>3</td><td>Device Supports LBA</td></tr> <tr><td>2</td><td>Directory of Services is Present</td></tr> <tr><td>1</td><td>Formatted Geometry Valid</td></tr> <tr><td>0</td><td>Reported Geometry Valid</td></tr> </tbody> </table>	Bit	Description	8-15	Reserved	7	Read Only	6	Generated Record	5	Use Reserved Area Boot Code Address	4	Configuration Time Stamp is valid	3	Device Supports LBA	2	Directory of Services is Present	1	Formatted Geometry Valid	0	Reported Geometry Valid
Bit	Description																					
8-15	Reserved																					
7	Read Only																					
6	Generated Record																					
5	Use Reserved Area Boot Code Address																					
4	Configuration Time Stamp is valid																					
3	Device Supports LBA																					
2	Directory of Services is Present																					
1	Formatted Geometry Valid																					
0	Reported Geometry Valid																					
6-9	DWord	Reported Cylinders																				
10-13	DWord	Reported Heads																				
14-17	DWord	Reported Sectors																				
18-21	DWord	Reported Bytes/Sector																				
22-29	QWord	Reported Sectors/Device																				
30-33	DWord	Formatted Cylinders																				
34-37	DWord	Formatted Heads																				
38-41	DWord	Formatted Sectors																				
42-45	DWord	Formatted Bytes/Sector																				
46-53	QWord	Formatted Sectors/Device																				
54-55	Word	BCD Year																				
56-57	Word	Linear Day																				
58-61	DWord	Configuration Time stamp																				
62	Byte	Reserved shall be 0																				
63	Byte	Device Index																				
64-71	QWord	Host Protected Area Start																				
72-79	QWord	Reserved Area Boot Code Address																				
80-81	Word	Number of entries in the BEER Directory of Services																				
82-83	Word	Length of a BEER Directory of Services Entry																				
84	Byte	Reserved shall be 0																				
85	Byte	Revision of the standard used to generate this record																				
86-125	String	Device Name																				
126-127	Word	16 Bit Checksum																				

### 5.2.1 Offset 0-1 (Signature Word)

An initial signature of BEEFh is placed in the sector to indicate BEER data present. If the BIOS or other software scans a portion of the media for BEER, this signature should be tested first.

### 5.2.2 Offset 2-3 (BEER Size)

The BEER size is the length of BEER in bytes. This is fixed at 128.

### 5.2.3 Offset 4-5 (Capabilities Word)

This word is a list of bit flags, which confirm the presence of all remaining BEER fields as well as device capabilities.

#### 5.2.3.1 Bit 7 (Read Only)

When this bit is set to one any writes to this sector shall not result in the data being changed. The INT 13h function used may or may not report an error.

#### **5.2.3.2 Bit 6 (Generated Record)**

When this bit is one the BEER record does not reside in the device, it is being generated by an outside source such as a BIOS or Option ROM.

#### **5.2.3.3 Bit 5 (Use Reserved Area Boot Code Address)**

If set to one and bit 2 (Directory of Services is Present) is set to zero the RABCA is valid. If the system fails to boot from the standard INT19h boot sector and calls INT 18h, then boot from the RABCA should be attempted. The service pointed to by the RABCA becomes the default Diagnostic Service.

#### **5.2.3.4 Bit 4 (Configuration Time Stamp is valid)**

Each time the BEER is updated all devices in the system shall have this bit set to one, and a time/date stamp is placed in bytes 54-61. This is one way for software to find new devices and deal with the associated issues. If the BIOS detects a device with a Configuration Time Stamp that is not within current system parameters, this means the system configuration has changed, or the device has been used in a different system. The BIOS may ask the user for a device number assignment, or the BIOS may defer to the operating system to make the drive letter/device assignment. This field is changed during boot when new devices are detected, or when devices are removed from the system. This time stamp is not changed in response to a BEER record update, such as adding or deleting a service area.

#### **5.2.3.5 Bit 3 (Device Supports LBA)**

If the device supports LBA, this bit shall be set to 1. When this bit is 1, the reported geometry (found at offset 6-29) may not be supplied. The formatted geometry (found at offset 30-53) shall be supplied if the conventional INT 13h interface addresses the device.

#### **5.2.3.6 Bit 2 (Directory of Services is Present)**

If BEER Directory of Services entries are present, this bit is set to one and bytes 80-83 contain valid data. The length of BEER is the product of the values in bytes 80-81 and bytes 82-83 plus the value in bytes 2-3. The first Beer Directory of Service entry starts immediately after the BEER header, where the length of the BEER exceeds the available space on the sector it is continued at the start of the preceding sector.

#### **5.2.3.7 Bit 1 (Formatted Geometry Valid)**

If geometry information is supplied in bytes 46-57 then this bit is set to 1. This bit shall only be zero if the conventional INT 13h interface does not support the device. Even if the device only supports LBA, a CHS geometry is still required for compatibility with the INT 13h functions described in this standard.

#### **5.2.3.8 Bit 0 (Reported Geometry Valid)**

If geometry information is supplied in bytes 22-33 this bit is set to 1. This geometry is usually derived from the device that accesses the media. If the device does not support CHS, this bit is 0

### **5.2.4 Offset 6-9 (Reported Cylinders)**

On ATA devices the contents of this field matches the contents of IDENTIFY DEVICE word 1. This is the total number of cylinders. The maximum cylinder number is one less because cylinder numbers start at 0.

### **5.2.5 Offset 10-13 (Reported Heads)**

On ATA devices the contents of this field matches the contents of IDENTIFY DEVICE word 3. This is the total number of heads. The maximum head number is one less. Head numbers start at 0.

### **5.2.6 Offset 14-17 (Reported Sectors)**

On ATA devices the contents of this field matches the contents of IDENTIFY DEVICE word 6. This is the total number of sectors per track. The maximum sector number is this number.

### **5.2.7 Offset 18-21 (Reported Bytes/Sector)**

This field is mandatory. On many devices, such as an ATA Hard Drive, this is fixed at 512 bytes. Other devices may use different sizes. For instance, CD-ROM sector sizes may vary from 2048 bytes to greater than 3000 bytes.

### **5.2.8 Offset 22-29 (Reported Sectors/Device)**

This field is mandatory. On ATA devices, the contents of this field matches the contents of IDENTIFY DEVICE words [61:60] if these words are valid. This value shall be greater than or equal to the product of Reported Cylinders (C), Reported Heads (H), and Reported Sectors (S). If the IDENTIFY DEVICE words [61:60] are not valid this field shall be the product of Reported Cylinders (C), Reported Heads (H), and Reported Sectors (S). In the case of an empty removable media device, this shall be the max value the device supports.

### **5.2.9 Offset 30-33 (Formatted Cylinders)**

This shall be the number of cylinders returned by INT 13h FN 08h and/or 48h when the user area is accessed. If conventional INT 13h addresses this device then Formatted Cylinders shall not exceed 1024.

### **5.2.10 Offset 34-37 (Formatted Heads)**

This shall be the number of heads returned by INT 13h FN 08h and/or 48h when the user area is accessed. If conventional INT 13h addresses this device then the number of Formatted Heads does not exceed 256.

### **5.2.11 Offset 38-41 (Formatted Sectors)**

This shall be the number of sectors per track returned by INT 13h FN 08h and/or 48h when the user area is addressed. If conventional INT 13h accesses this device then Formatted Sectors shall not exceed 63.

### **5.2.12 Offset 42-45 (Formatted Bytes/Sector)**

This field is mandatory. On many devices, such as the ATA Hard Drive, this is fixed at 512 bytes. Other devices may use different sizes. For instance, CD-ROM sector sizes may vary from 2048 bytes to greater than 3000 bytes. It is possible for geometric translation to change the sector size. This means the "Formatted Bytes/Sector" may be different than the "Reported Bytes/Sector".

### **5.2.13 Offset 46-53 (Formatted Sectors/Device)**

This field is mandatory. Formatted Sectors/Device is the total number of addressable sectors. If the formatted geometry is valid, Formatted Sectors shall be great than or equal to the space addressed by the geometry.

### **5.2.14 Offset 54-55 (BCD Year)**

This word describes the year in Binary Coded Decimal (BCD) format (yyyy) when the BEER was last updated.

### **5.2.15 Offset 56-57 (Linear Day)**

This word is Linear Calendar date, that is the number of days after December 31st – 1. See section 5.2.14 for a description of the year.

### **5.2.16 Offset 58-61 (Configuration Time Stamp)**

This is the number of seconds past midnight of the date specified in 5.2.14 and 5.2.15 when this record was last updated.

### **5.2.17 Offset 63 (Device Index)**

This field is mandatory. Device Index is the number that INT 13h uses to access the device. Traditionally, mass storage devices have been 80h and above. If this field is FFh, the device number shall be assigned

dynamically.

### 5.2.18 Offset 64-71 (Host Protected Area Start)

This field specifies the first sector of the Host Protected Area. This is the max address +1

### 5.2.19 Offset 72-79 (Reserved Area Boot Code Address)

If bit 5 of the Capabilities word at byte 4 is one and bit 2 of the capabilities word is cleared to 0, this field specifies the absolute address of the " Reserved Area Boot Sector". When the Reserved Area Boot Code Address (RABCA) is active, BEER extended INT 19h loads the sector at the supplied address into memory at 0:7C00h. INT 19h shall then jump to 0:7C00h and begin the load process. The whole of the Host Protected Area excluding the BEER is considered to be one service area. The RABCA is within the Service Area.

### 5.2.20 Offset 80-81 (Number of entries in the BEER Directory of Services)

If bit 2 of the Capabilities word at offset 4 is 1, this field specifies the number of entries in the BEER Directory.

### 5.2.21 Offset 82-31 (Length of a BEER Directory of Service Entry)

If bit 2 of the Capabilities word at offset 4 is 1, this field specifies the number of bytes in a BEER Directory table entry. This number shall be set to 64.

### 5.2.22 Offset 85 (Revision of the standard used to generate this record)

This is the PARTIES revision level used to describe the BEER sector. The first BCD digit is the major revision number; the second BCD digit is the minor revision number.

### 5.2.23 Offset 86-125 (Device Name)

This is a null terminated string that is suitable for display to the user. If the string is 40 characters the null is not present. This string shall only be made up of printable ASCII characters (ASCII 20h-7Eh).

### 5.2.24 Offset 126-127 (16 Bit Checksum)

The data structure checksum is the two's complement of the sum of all words from byte offset 0 through byte offset 124. Each word shall be added with unsigned arithmetic, and overflow shall be ignored. The sum of all 64 words shall be zero.

## 5.3 BEER Directory of Services Description

BEER Directory of Services is LBA based and is BIOS readable. This eliminates the need for boot code when a system is updated to work with BEER. Each service area is designed to have a string that is suitable for display to a user. This gives the BIOS the ability to present a meaningful name when the user accesses a given service area. The only constraint on the number of directory entries (one per service area) is the size of the media. The four-entry limit of the conventional partition table does not apply to this standard. The remainder of this section describes BEER Directory of Service Entries. Table 2 defines the BEER Directory of Services Entry structure.

Table 2 - BEER Directory of Services Entry

Offset	Type	Description												
0	Byte	<p style="text-align: center;">Directory Flags</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Bit</th><th>Description</th></tr> </thead> <tbody> <tr> <td>7</td><td>Service area is available as B:</td></tr> <tr> <td>6</td><td>Reserved</td></tr> <tr> <td>5</td><td>Diagnostic Service</td></tr> <tr> <td>4</td><td>Service Area is Read Only</td></tr> <tr> <td>3</td><td>This Boot</td></tr> </tbody> </table>	Bit	Description	7	Service area is available as B:	6	Reserved	5	Diagnostic Service	4	Service Area is Read Only	3	This Boot
Bit	Description													
7	Service area is available as B:													
6	Reserved													
5	Diagnostic Service													
4	Service Area is Read Only													
3	This Boot													

Offset	Type	Description		
		2	Empty Service Area	
		1	Hidden Service Area	
		0	Service Area is bootable as A:	
1	Byte	Reserved.		
2-9	QWord	Service Area Start		
10-17	QWord	Service Area Size		
18-21	DWord	Load Sectors		
22-25	DWord	Load Address		
26-27	Word	Service Area ID		
28-59	Byte	ID String		
60-61	Word	Reserved		
62-63	Word	16 bit Checksum.		

### 5.3.1 Offset 0 (Directory Flags)

The directory flags are a bit map, that enables several different boot options and provide some data security.

#### 5.3.1.1 Bit 7 (Service Area Is Available as B)

When this bit is one the service area shall be visible as drive B:, permitting boot from a normal drive A: diskette or drive C:. This is useful when installing an operating system in the service area. This bit shall be cleared when the service area is bootable.

#### 5.3.1.2 Bit 5 (Diagnostic Service)

This bit shall be set to one when the Service Area contains a Diagnostic Service. In the event that diagnostic services are required the BIOS shall scan the Directory of Service Entries starting at the first entry after the BEER header. The first entry found with both bit 0 and bit 3 set to one shall be chosen as the diagnostic service to boot.

#### 5.3.1.3 Bit 4 (Service Area is Read Only)

When this bit is set to one no data shall be written to this Service Area. This field is intended as a user flag and shall be enforced by the OS as well as the BIOS. It is possible for the user to set this bit to 0, write new data to the service area, and set the bit back to 1.

#### 5.3.1.4 Bit 3 (This Boot)

When this bit is set to one the Service Area has been designated as the boot area. Extended INT 19h chooses this Service Area to boot from instead of the User Area during the normal boot sequence if the user has selected a diagnostic boot.

#### 5.3.1.5 Bit 2 (Empty Service Area)

When this bit is set to one the Service Area has been reserved and is not available for re-use. The BIOS shall disregard this Service Area regardless of what other options may be active.

#### 5.3.1.6 Bit 1 (Hidden Service Area)

When this bit is set to one the BIOS shall not present this service area to the user and shall ignore this Service Area. Software shall not expose this Service Area to the user.

#### 5.3.1.7 Bit 0 (Service Area is Bootable)

When this bit is one the service area is a candidate for booting at the users option. If this bit is 0, the BIOS shall not present this service area to the user unless the Service Area Is Available as B: bit is set, see

5.3.1.1.

### 5.3.2 Offset 2-9 (Service Area Start)

This is the address of the first sector in the Service Area. When the BIOS boots this service area, sectors are loaded starting at this address.

### 5.3.3 Offset 10-17 (Service Area Size)

This is the number of sectors allocated to the service area.

### 5.3.4 Offset 18-21 (Load Sectors)

This is the number of sectors the BIOS loads to boot the system.

### 5.3.5 Offset 22-25 (Load Address)

This is the 64-bit linear host memory address. The conventional address is 31,744 (0:7C00h). BEER Directory of Services allow any address to be specified. If the address is above the 1MB boundary the service area shall have Directory Flags bit 1 set to one. This address is not SEG:OFFSET, it is a 64 bit linear address. This means that A000h:0 is represented as A0000h, or 655,360.

### 5.3.6 Offset 26-27 (Service Area ID)

The Service Area ID is used to enable Different System Vendor codes to be placed on the Device. The ID shall be the same code allocated to a vendor for the purposes of PCI identification. If the vendor does not have a PCI identification number then this field is cleared to 0. A combination of the vendor ID and the ID string (see 5.3.7) may uniquely identify the source and function of the content of the Host Protected Area. For example, a device manufacturer may place diagnostic code in a service area. The system manufacturer may then add a recovery process to another service area.

### 5.3.7 Offset 28-59 (ID String)

The ID string is a null terminated ASCII string, which is displayed to the user by the BIOS, OS or other software as the name of the service area. If the string is 22 characters the null is not present.

### 5.3.8 Offset 62-63 (16 Bit Checksum)

The data structure checksum is the two's complement of the sum of all words from byte offset 0 through byte offset 60. Each word shall be added with unsigned arithmetic, and overflow shall be ignored. The sum of all 32 words shall be zero.

## 6 Runtime Services

The Runtime Services described in the following sections are defined for the purposes of providing an emulated device by the BIOS. Runtime services provided by a system BIOS for operating mass storage devices are beyond the scope of this standard (see BIOS Enhanced Disk Drive Services (EDD) T13/1386D).

### 6.1 INT 13h Dispatcher

Runtime support for the services running within a Service Area shall be achieved by hooking the INT 13h BIOS interrupt service. This gives the handler access to all commands issued to the BIOS disk subsystem. The handler shall also hook INT 40h to gain access to the floppy subsystem. The following INT 13h functions are defined to show how each function shall respond when reporting a floppy drive.

### 6.2 Reset

In	Description
AH	00h

<b>DL</b>	Device number
<b>Out</b>	<b>Description</b>
AH	00h
Carry Flag	Clear

The Reset function shall always return success, while issuing no commands to the device

### 6.3 Get Status

<b>In</b>	<b>Description</b>
AH	01h
<b>Out</b>	<b>Description</b>
AL	Status of last command executed

Return the status of the last INT 13h/40h function call.

### 6.4 Read Sectors

<b>In</b>	<b>Description</b>
AH	02h
AL	Number of sectors to read
CH	Lower eight bits of the number of cylinder number
CL	Bits <5,0> Sectors number, Bits <7,6> Most significant bits of the cylinder number
DH	Head
DL	Device
ES:BX	Start address of the buffer to fill
<b>Out</b>	<b>Description</b>
AH	Status of command executed
AL	Number of sectors read
ES:BX	Filled buffer
Carry Flag	Set if error

The Read Sectors function transfers data from the Boot Code Area on the device to a buffer supplied by the caller.

Change Address from CHS to LBA using the following formula:

$$\text{LBA} = (C_1 * H_0 + H_1) * S_0 + S_1 - 1 + \text{BCA}$$

Where:

- C<sub>1</sub> = Selected Cylinder Number
- H<sub>0</sub> = Number of Heads (Maximum Head Number + 1)
- H<sub>1</sub> = Selected Head Number
- S<sub>0</sub> = Maximum Sector Number
- S<sub>1</sub> = Selected Sector Number
- BCA = Boot Code Address

## 6.5 Write Sectors

In	Description
AH	03h
AL	Number of sectors to write
CH	Lower eight bits of the cylinder number
CL	Bits <5,0> Sector number, Bits <7,6> Top two bits of the cylinder number
DH	Head
DL	Device
ES:BX	Start of the buffer to write
Out	Description
AH	Status of command executed
AL	Number of sectors written
Carry Flag	Set if error

The Write Sectors function transfers data from a buffer to the Boot Code Area on the device.

Change Address from CHS to LBA using the following formula:

$$LBA = (C_1 * H_0 + H_1) * S_0 + S_1 - 1 + BCA$$

Where:

$C_1$  = Selected Cylinder Number

$H_0$  = Number of Heads (Maximum Head Number + 1)

$H_1$  = Selected Head Number

$S_0$  = Maximum Sector Number

$S_1$  = Selected Sector Number

BCA = Boot Code Address

## 6.6 Verify Sectors

In	Description
AH	04h
AL	Number of sectors to verify
CH	Lower eight bits of the cylinder number
CL	Bits <5,0> sector number, Bits <7,6> Top two bits of the cylinder number
DH	Head
DL	Device
Out	Description
AH	00h
AL	Number of sectors verified
Carry Flag	Clear

The Verify Sectors function causes the device to check all the sectors in the specified range. If the device is unable to read one or more of the sectors without error, this function returns carry set.

## 6.7 Format Track

In	Description
AH	05h
AL	Number of sectors to create on this track
CH	Track
CL	Sector
DH	Head
DL	Device
ES:BX	Array of 4-byte address fields
Byte 0	Track
Byte 1	Head
Byte 2	Sector
Byte 3	Bytes per sector 0=128, 1=256, 2=512, 3=1024
Out	Description
AH	Status of command executed
Carry Flag	Set if error

The Format Track function shall always return success, while issuing no commands to the device

## 6.8 Get Device Parameters

In	Description
AH	08h
DL	Device
Out	Description
AH	Status of command executed
BL	Device Type: 10h
DL	Number of INT 40h devices
DH	Maximum value for head number
CL	Maximum value for sector number (bits <0,5>)
CH	Maximum value for cylinder number
ES:DI	Pointer to device parameter table
Carry Flag	Clear

The Get Device Parameters function returns a device type of 10h. This informs the caller that the media does not conform to conventional floppy standards.

## 6.9 Get Current Device Parameters

In	Description
AH	15h
DL	Device
Out	Description
AH	02=Change detection supported

Get Current Device Parameters always returns Change Detection Support for the Service Area.

## 6.10 Get Device Change Status

In	Description
AH	16h
DL	Device
Out	Description
AH	00=No disk change, 06=Disk has changed

Since this is a hard disk and a floppy drive is being emulated, this function shall always return 0.

## 6.11 Set Device Type

In	Description
AH	17h
AL	Disk Type 00 - reserved 01 - 48-tpi media, DD drive 02 - 48-tpi media, HD drive 03 - 96-tpi media, HD drive 04 - 135-tpi media
DL	Device
Out	Description
N/A	No information passed on exit

The Set Device Type function shall always return success, while issuing no commands to the device

## 6.12 Set Media Type for Format

In	Description
AH	18h
CH	Lower eight bits of number of tracks
CL	Bits <5,0> Sectors per Track, Bits <7,6> Top two bits of number of tracks
DL	Device
Out	Description
AH	00=Requested combination supported 0C=Not supported or device type unknown 80=No media present
ES:DI	Disk parameter table

The Set Media Type for Format command shall return 00h, requested combination supported if the parameters in CH and CL fit within the Service Area. Otherwise, return Carry set, AH = 0Ch.

### 6.13 Sense Media Type

In	Description
AH	20h
DL	Device
Out	Description
AL	Media Type: 10h=Other Media Device
AH	Media present: 00h=Media present
Carry flag	Clear

Always return AL = 10h and AH=0

### 6.14 Check Extensions Present

In	Description										
AH	41h										
BX	55AAh										
DL	Device										
Out	Description										
AL	Internal Use, not preserved										
AH	21h, Major version of these extensions										
BX	AA55h										
CX	<p style="text-align: center;">Interface Support Bit map</p> <table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>3-15</td> <td>Reserved</td> </tr> <tr> <td>2</td> <td>EDD Support</td> </tr> <tr> <td>1</td> <td>Device Locking and Ejecting</td> </tr> <tr> <td>0</td> <td>Extended access functions</td> </tr> </tbody> </table>	Bit	Description	3-15	Reserved	2	EDD Support	1	Device Locking and Ejecting	0	Extended access functions
Bit	Description										
3-15	Reserved										
2	EDD Support										
1	Device Locking and Ejecting										
0	Extended access functions										
Carry flag	Clear if INT 13h, FN 41h supported										

The Check Extensions Present function notifies the caller that Extended device support is preset. See BIOS Enhanced Disk Drive Services (EDD) T13/1386D for a full definition. If CX is set to zero on return then INT 13h FN 48h is the only function that shall be supported

### 6.15 Get Device Parameters

In	Description
AH	48h
DL	Device
DS:SI	Address of result buffer. See Table 3 for data format
Out	Description
AH	Status of command executed
DS:SI	Result Buffer
Carry flag	Set if error

This function is mandatory regardless of the interface subset that is supported. The geometry returned by Get Device Parameters is the same as was reported by function 08h and reflects the size of the service area.

Table 3 - Result Buffer

Offset	Type	Description																		
0	Word	The caller sets this value to the maximum buffer length in bytes. If the length of this buffer is less than 30 bytes, this function does not return the pointer to DPT extension. If the buffer length is 30 or greater on entry, it shall be set to 30 on exit. If the buffer length is between 26 and 29, it shall be set to 26 on exit. If the buffer length is less than 26 on entry an error shall be returned.																		
2	Word	<p><b>Information Flags</b></p> <p>In the following table, a bit set to one indicates that the feature is available; a bit cleared to zero indicates the feature is not available and shall operate in a manner consistent with the conventional INT 13h interface.</p> <table border="1"> <thead> <tr> <th>Bit</th><th>Description</th></tr> </thead> <tbody> <tr> <td>0</td><td>DMA boundary errors are handled transparently</td></tr> <tr> <td>1</td><td>The geometry supplied in bytes 4-15 is valid</td></tr> <tr> <td>2</td><td>Device is removable</td></tr> <tr> <td>3</td><td>Device supports write with verify</td></tr> <tr> <td>4</td><td>Device has change line support (bit 2 shall be set to one)</td></tr> <tr> <td>5</td><td>Device is lockable (bit 2 shall be set to one).</td></tr> <tr> <td>6</td><td>Device geometry is set to maximum, no media is present (bit 2 shall be set to one). This bit is turned off when media is present in a removable media device.</td></tr> <tr> <td>7-15</td><td>Reserved, shall be 0</td></tr> </tbody> </table>	Bit	Description	0	DMA boundary errors are handled transparently	1	The geometry supplied in bytes 4-15 is valid	2	Device is removable	3	Device supports write with verify	4	Device has change line support (bit 2 shall be set to one)	5	Device is lockable (bit 2 shall be set to one).	6	Device geometry is set to maximum, no media is present (bit 2 shall be set to one). This bit is turned off when media is present in a removable media device.	7-15	Reserved, shall be 0
Bit	Description																			
0	DMA boundary errors are handled transparently																			
1	The geometry supplied in bytes 4-15 is valid																			
2	Device is removable																			
3	Device supports write with verify																			
4	Device has change line support (bit 2 shall be set to one)																			
5	Device is lockable (bit 2 shall be set to one).																			
6	Device geometry is set to maximum, no media is present (bit 2 shall be set to one). This bit is turned off when media is present in a removable media device.																			
7-15	Reserved, shall be 0																			
4	Double Word	Number of physical cylinders. This is one greater than the maximum cylinder number. Use INT 13h Fn 08h to find the logical number of cylinders.																		
8	Double Word	Number of physical heads. This is one greater than the maximum head number. Use INT 13h Fn 08h to find the logical number of heads.																		
12	Double Word	Number of physical sectors per track. This number is the same as the maximum sector number for any given track because sector addresses are one based. Use INT 13h Fn 08h to find the logical number of sectors per track.																		
16	Quad Word	Number of physical sectors in the Service Area.																		
24	Word	Number of bytes in a sector.																		
26	Double Word	Pointer to Enhanced Disk Drive (EDD) configuration parameters. This field is only present if INT 13h, Fn 41h, CX register bit 2 is enabled. This field points to a temporary buffer that the BIOS may re-use on subsequent INT 13h calls. A value of FFFFh:FFFFh in this field means that the pointer is invalid.																		



white paper

## ImageCast MFG/Area51/PXE Integration

## Contents

Revision History.....	3
Disclaimer .....	3
<b>1 Abstract .....</b>	<b>3</b>
<b>2 Terminology .....</b>	<b>3</b>
2.1 Area51 terminology.....	3
2.2 Imaging terminology.....	4
2.3 Standalone “pull” or “push” .....	4
<b>3 Overview of the integration process .....</b>	<b>4</b>
<b>4 Installing and creating necessary components .....</b>	<b>5</b>
4.1 Setting up the StorageSoft PXE Server.....	5
4.2 Creating diskettes for Area51, mapping a network drive or PC diagnostics .....	5
4.3 Setting up the boot images for use with the PXE Server.....	5
<b>5 Implementing manufacturing processes from the PXE Server .....</b>	<b>7</b>
5.1 Using Area51 for PC diagnostics .....	7
5.2 Using ImageCast MFG via PXE.....	8
5.3 Using Area51 for imaging via PXE and disaster recovery.....	9
<b>6 Conclusion .....</b>	<b>10</b>
<b>7 Contact information .....</b>	<b>10</b>

## Revision History

Date	Updated By	Version	Changes
07/25/01	Narayan Khalsa	1.0	Initial Creation

## Disclaimer

*All proprietary terms in this document are trademarks of StorageSoft, Inc. and may not be used by any third parties without indication of such ownership (by use of the trademark symbol ™).*

*The information presented in this document is to be considered the "best advice" our organization has to offer, however there is no warranty—implied or otherwise—that the given information will give predictable results under any conditions. By applying the information presented here, the reader is making an agreement to accept any and all responsibility of actions taken, based upon said information. The reader also agrees to hold StorageSoft, Inc., as well as its agents, representatives, partners and affiliates harmless in the event that applying said information results in manifest damages of a real or conceptual nature.*

## 1 Abstract

StorageSoft has developed a suite of utilities known as Area51, PXE Server and ImageCast MFG that can be combined to provide manufacturers, BTO/CTO providers and system builders with a complete manufacturing process for imaging PCs. It is possible to merge StorageSoft's current hard drive imaging technology and Protected Area technology with PXE technology to create an automated assembly line process that provides imaging and disaster recovery to the end customer. This process eliminates many of the time-consuming steps PC builders are using today.

## 2 Terminology

### 2.1 Area51 terminology

This list defines terms related to the Area51 product.

Address (LBA)	A method of addressing the sectors on a hard drive in a linear format. Hard drives generally contain millions of sectors. These sectors are where the data is stored on the drive. LBA simply maps each sector out in a linear manner; the first sector on the drive is LBA 0, the second sector is LBA 1, etc.
BIOS Engineering Extension Record (B.E.E.R.)	A data structure located in the last sector of the drive that contains information about the <u>Protected Area</u> and <u>Directory of Services</u> . The ATA SETMAX Address command hides this structure.
Directory of Service (DoS)	A BIOS readable string contained in the BEER that allows the BIOS to present a meaningful name for each serviceable area available to the user once the Protected Area is accessed.
IDE/ATAPI	Area51 and the concept of a Protected Area are currently only available on IDE/ATAPI type hard drives. Hard drive manufacturers may add SCSI support in the future.
Protected Area	The reserved and protected space on the hard drive not normally accessible to the user. While booted to the Operating System, the Protected Area is completely hidden and inaccessible.
SETMAX Address	The ATA command that, when sent to the drive, sets the last addressable sector in the user area. Generally, this command is used to reduce the total capacity of a hard drive when first initiated in order to create the Protected Area.
User Area	The area of the hard disk that is available to users. <u>The user area is where the Operating System, Application programs, and user-stored files reside.</u>

## 2.2 Imaging terminology

This list defines terms used in the Imaging industry.

<b>Application Imaging</b>	The use of snapshot technology to capture the installation of an application on an operating system to a file. This file can then be deployed to any machine with the same operating system as a means of installing the application. It may also be merged with a base image of the same operating system during the imaging process.
<b>Drive Imaging</b>	In simplest terms, Disk Imaging or Hard Drive “Cloning” is the process whereby an exact “image” of a PC hard drive is created and then copied via a network to one or many similarly configured target PC systems. This disk image is effectively an exact picture of the model drive including all files that make up the operating system, applications, configuration settings, hardware drivers, etc. Disk Imaging then replicates this exact picture to multiple PCs across a network.
<b>Image Layering</b>	The term used to describe the process of merging images of applications into base images of model systems.
<b>Model System</b>	A PC that has been set up for the purpose of creating an image for deployment to other PCs.
<b>Post Configuration</b>	The process of configuring a PC after an image has been deployed to a PC.

## 2.3 Standalone “pull” or “push”

<b>Standalone “Pull” or “Push” technology</b>	The process of restoring or creating an image file from a mapped network drive or local media device.
---	---

## 3 Overview of the integration process

In most manufacturing environments, the process of building a PC starts with assembling the hardware, but much more needs to happen before the PC is ready to ship. This document will outline the process of automating the manufacturing of a PC—from the assembly line to shipping—by employing software developed by StorageSoft, Inc.

Once the hardware is assembled, the PC needs all hardware to be tested prior to installing any software to ensure that there are no defective components. By booting the machine via the StorageSoft PXE Server, a scripted process can be used to run diagnostic programs either locally on the PC or remotely from a server. Scripting the creation of a partition or a Protected Area and then installing diagnostic software into the partition or area can run the local PC portion.

Once the PC has completed the diagnostic stage, two scenarios are possible—the Protected Area or partition can be removed, leaving the drive in its original state, or the Protected Area can be retained and used as a disaster recovery solution by using Area51 and the ImageCast Restore product.

In the first scenario, the Protected Area can be removed through simple DOS scripting. If desired, upon completion of diagnostics, the machine can be rebooted to a second boot image that facilitates the imaging process, which installs all necessary software and can even customize each machine’s individual settings (network settings, desktop settings, etc.).

In the second scenario, the image can be copied into the Protected Area to be used for disaster recovery once the image has been deployed. In this manner, a scripted process can facilitate each step on the assembly line from the time the hardware is assembled until the PC is ready to be packaged and shipped.

## 4 Installing and creating necessary components

### 4.1 Setting up the StorageSoft PXE Server

Install the PXE Server on a Windows NT or 2000 Server. Note that there must also be a DHCP Server on the network, preferably the same machine on which the PXE Server is installed. For more information on installing the PXE Server, see the *ImageCast PXE Server White Paper* located on our website at <http://www.storagesoft.com> (Products - ImageCast).

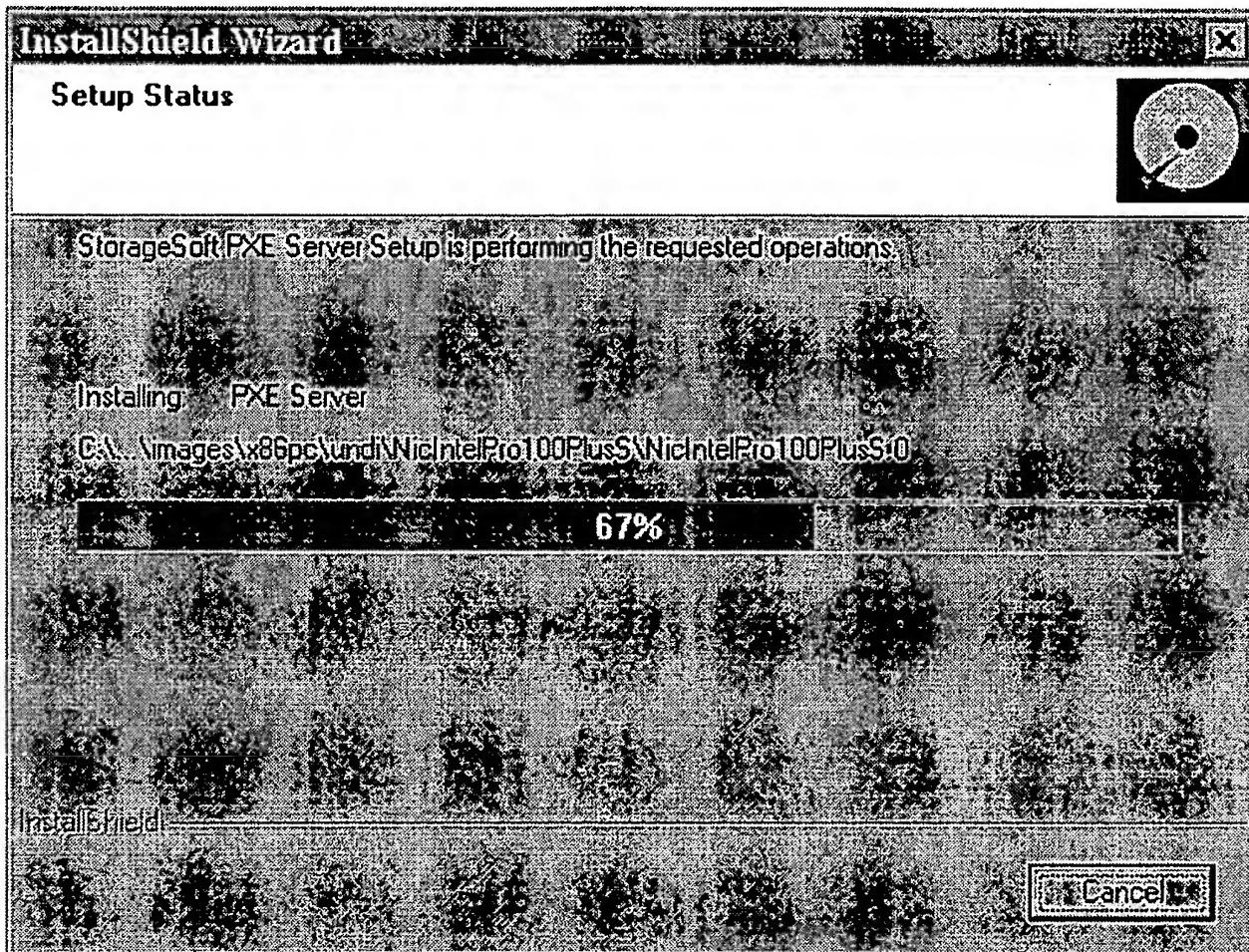


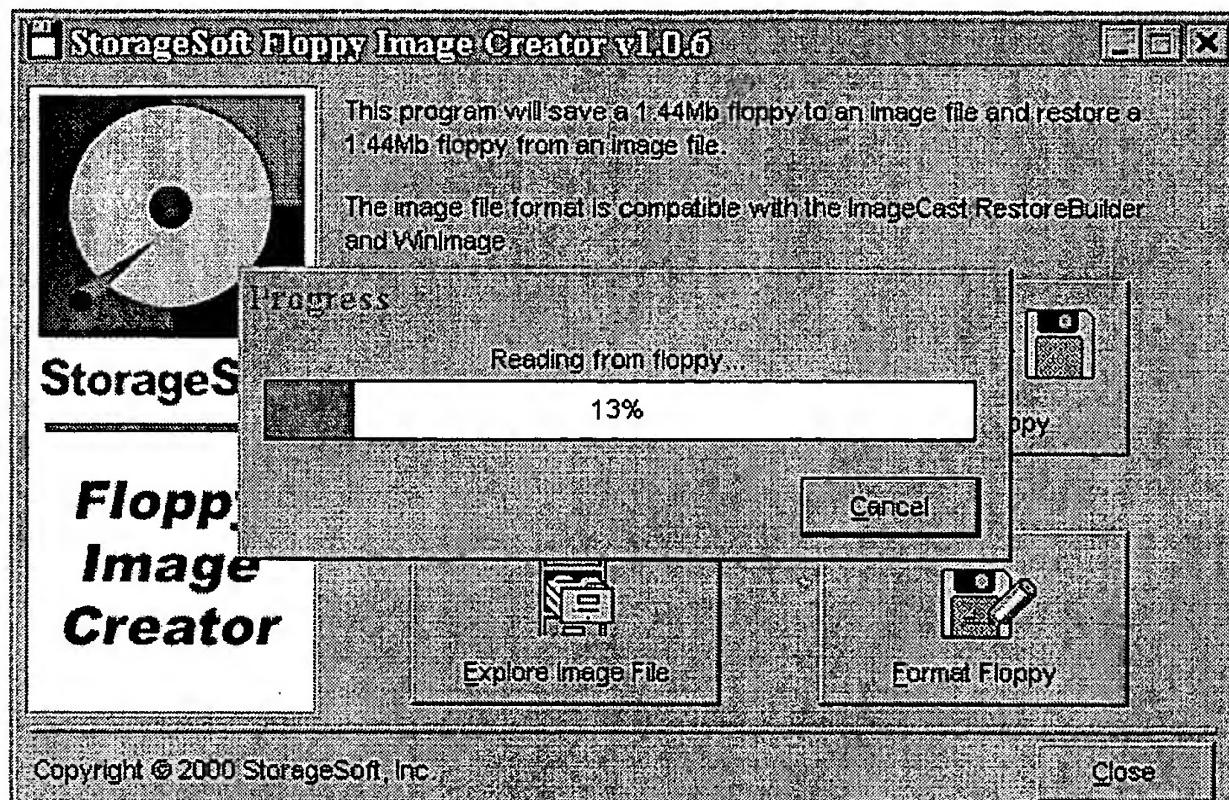
Figure 1 PXE Server InstallShield Wizard

### 4.2 Creating diskettes for Area51, mapping a network drive or PC diagnostics

Use the Area 51 Setup Wizard to create a bootable floppy diskette that will create a Protected Area on the hard drive and copy the necessary files for PC Diagnostics or imaging the PCs with an operating system. The wizard allows the creation of one or multiple services (Service Areas) within the Protected Area. For more information on this, please see the *Area51 White Paper* or the *Area51 Tutorial* on our website at <http://www.storagesoft.com/sbs>. If you are using ImageCast ClientBuilder, you can create a mapped network boot diskette that will allow you to connect remotely to a network drive and run diagnostics, imaging tools or creation of a Protected Area from the network drive. You can also create a boot diskette to launch PC diagnostics to verify hardware integrity prior to imaging or shipping a PC.

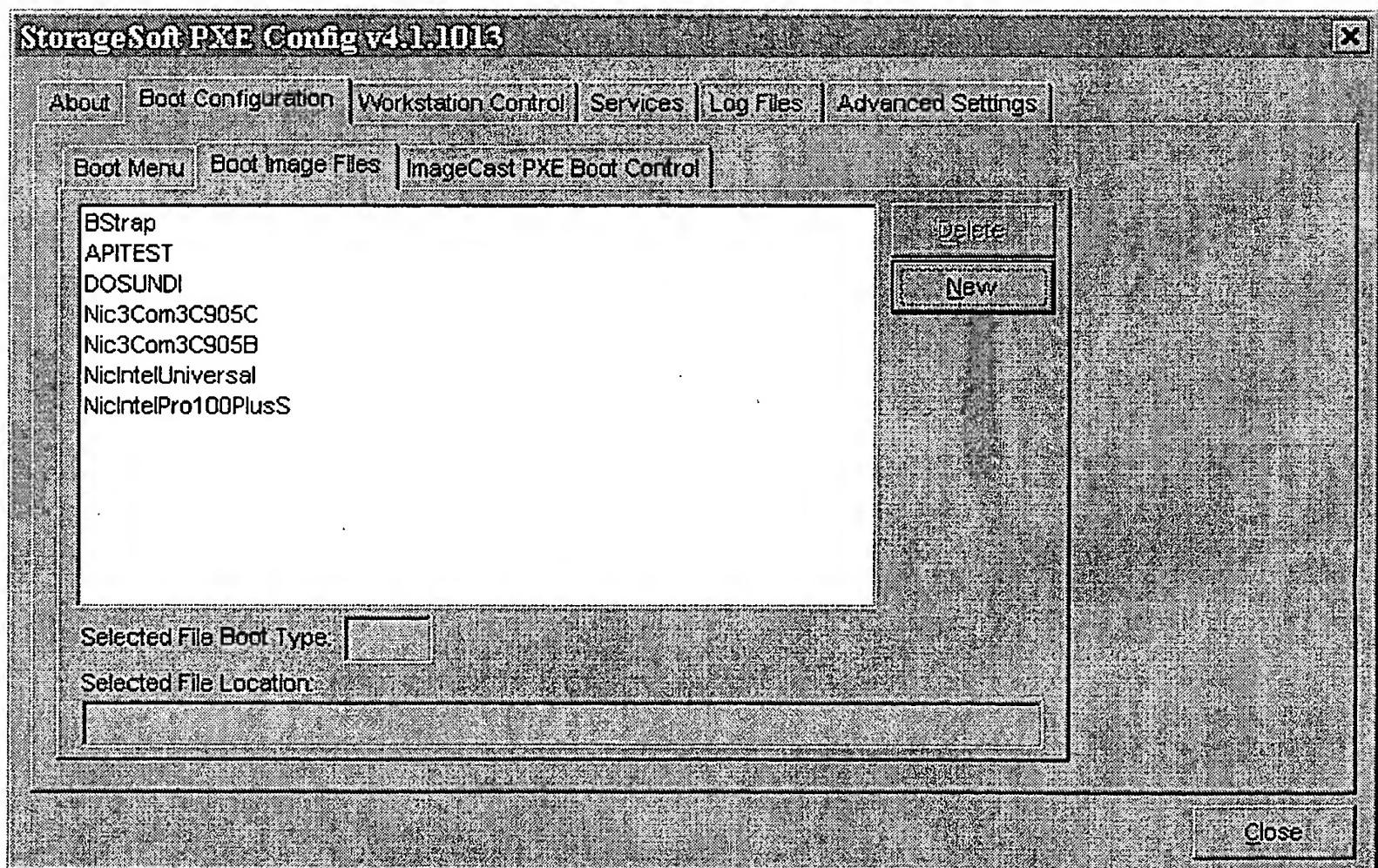
### 4.3 Setting up the boot images for use with the PXE Server

Once you have installed the PXE Server and created the boot diskettes, you are now ready to use the Floppy Image Creator program to create boot images for using Area51, diagnostics software and/or ImageCast MFG. Using the StorageSoft Floppy Image Creator, you can easily read a floppy diskette and turn it into a boot image file (see Figure 2 ).



**Figure 2 Creating a floppy image file**

These boot images can then be imported into the StorageSoft PXE Server (see Figure 3 ) and added to the boot menu or selected automatically from the PXE config to use one boot image and then revert to another upon the next reboot (see Figure 4 ). See "Using Area51 for PC diagnostics" on page 7 regarding implementing the boot menu options as necessary based on the scenario that applies to your implementation.



**Figure 3 Adding a boot image file to the PXE server**

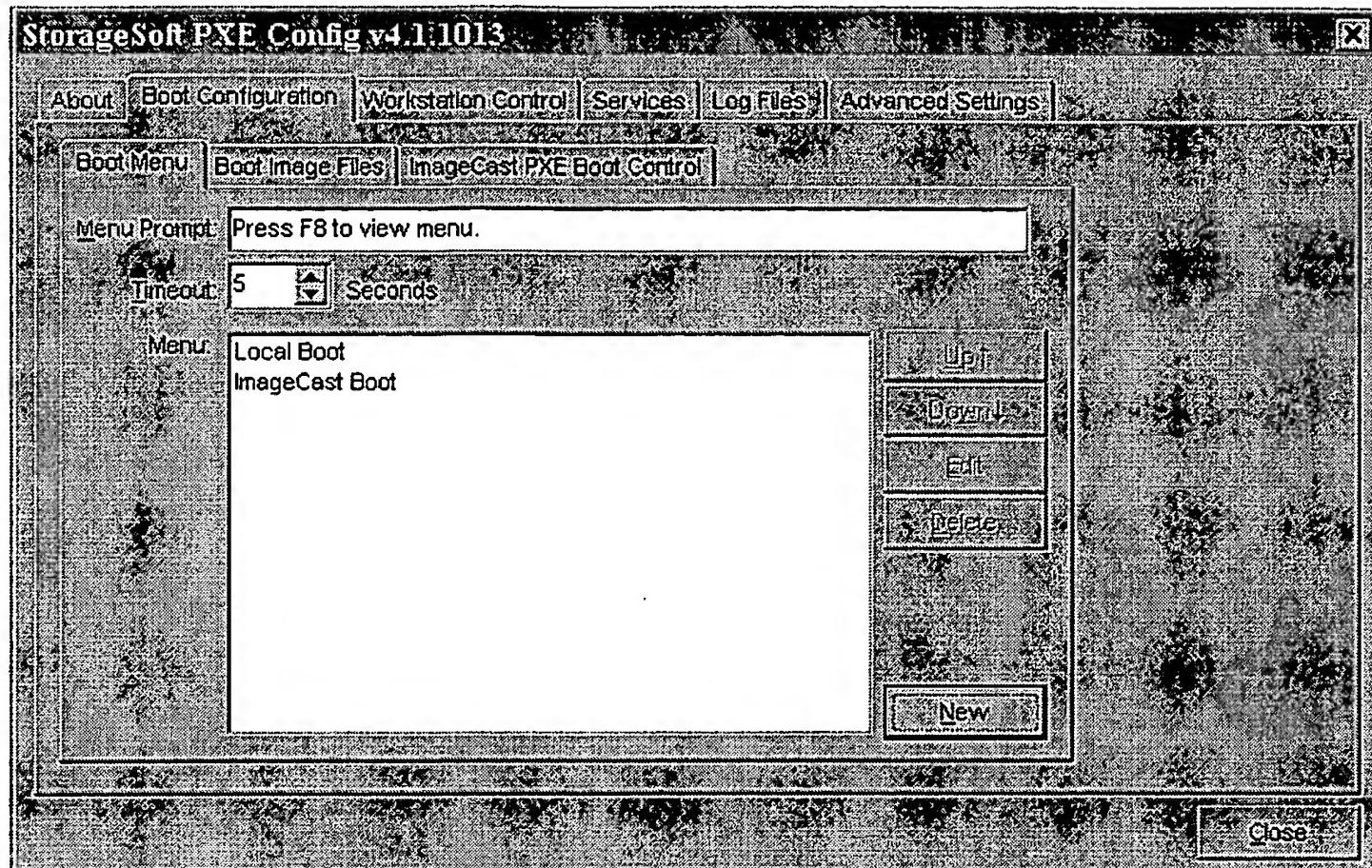


Figure 4 Adding a boot menu item with PXE config

## 5 Implementing manufacturing processes from the PXE Server

This section discusses the different applications of these boot images on a manufacturing floor. Keep in mind that these processes are recommendations and have numerous variations for different manufacturing environments. As such, they are presented as three general scenarios to explain the basic operation of Area51 and ImageCast MFG in a manufacturing environment.

### 5.1 Using Area51 for PC diagnostics

In this scenario, Area51 is being used to run diagnostics on a drive that has already been imaged but requires that the hardware assembled on the manufacturing line be tested prior to shipment of the PC.

First, create a boot image for the PXE server to launch Area51 either via the boot image or from a network drive. From this boot image, a scripted process can be used to set up the Protected Area with one or many services. This scripted process can also include the copying of files into the Protected Area from a mapped network drive, CD-Rom drive or any DOS drive letter. In most cases, PC diagnostics will not fit onto a floppy and will need to be copied into Area51 in order to be executed. The scripted process can then facilitate the PC rebooting into the Protected Area to launch the PC diagnostics and generate the appropriate log files to verify that the hardware passed the diagnostics successfully.

Once the diagnostics are complete, the log files can be copied to a network share for verification purposes. Finally, a boot image can be selected to remove Area51 from the drive, returning the drive to its original state. The PC is now ready for shipping. The following screen shot shows the Area51 program as it would appear for a manual creation of the Protected Area.

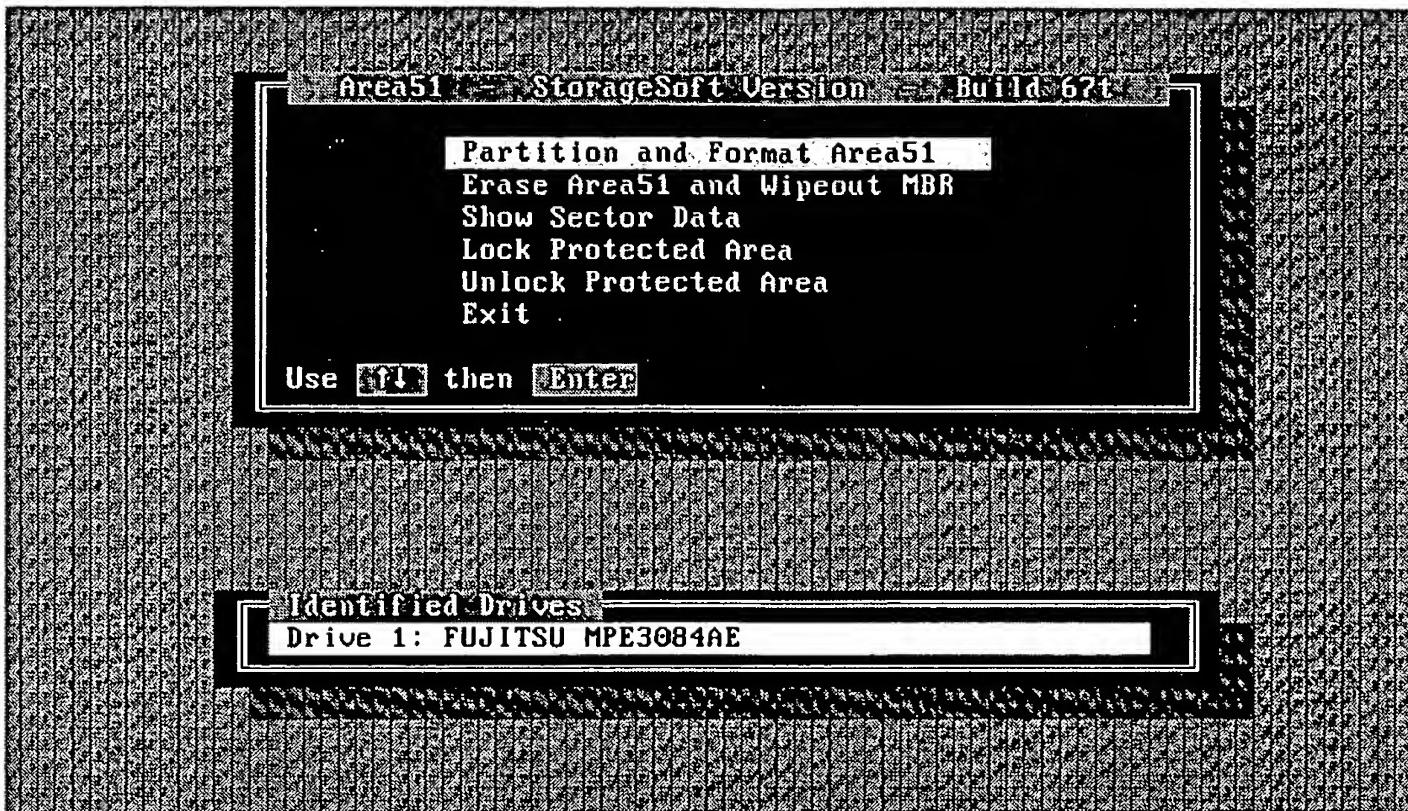


Figure 5 Menu for manual creation of Area51

## 5.2 Using ImageCast MFG via PXE

In this scenario, the PC has been through PC diagnostics and is ready to be imaged with an operating system before being shipped to the customer. The boot Image created from the ImageCast ClientBuilder will map a network drive and launch the ImageCast client file with command line switches or with a scripted process that will restore an image from the mapped network drive to the PC.

A log file can be generated to report success of the client or any errors that may have occurred. In the case of failure, the client file adheres to DOS error level reporting. The scripted process can include steps to run from DOS after an imaging failure. In the case of successful imaging, the PXE server can be set to revert to a local boot; the PC is booted into the OS and is ready to be shipped. The following screen shot shows the ImageCast client dialog during an imaging process. This dialog box can be altered using RestoreBuilder to display specific customer information, or it can be used as shown.

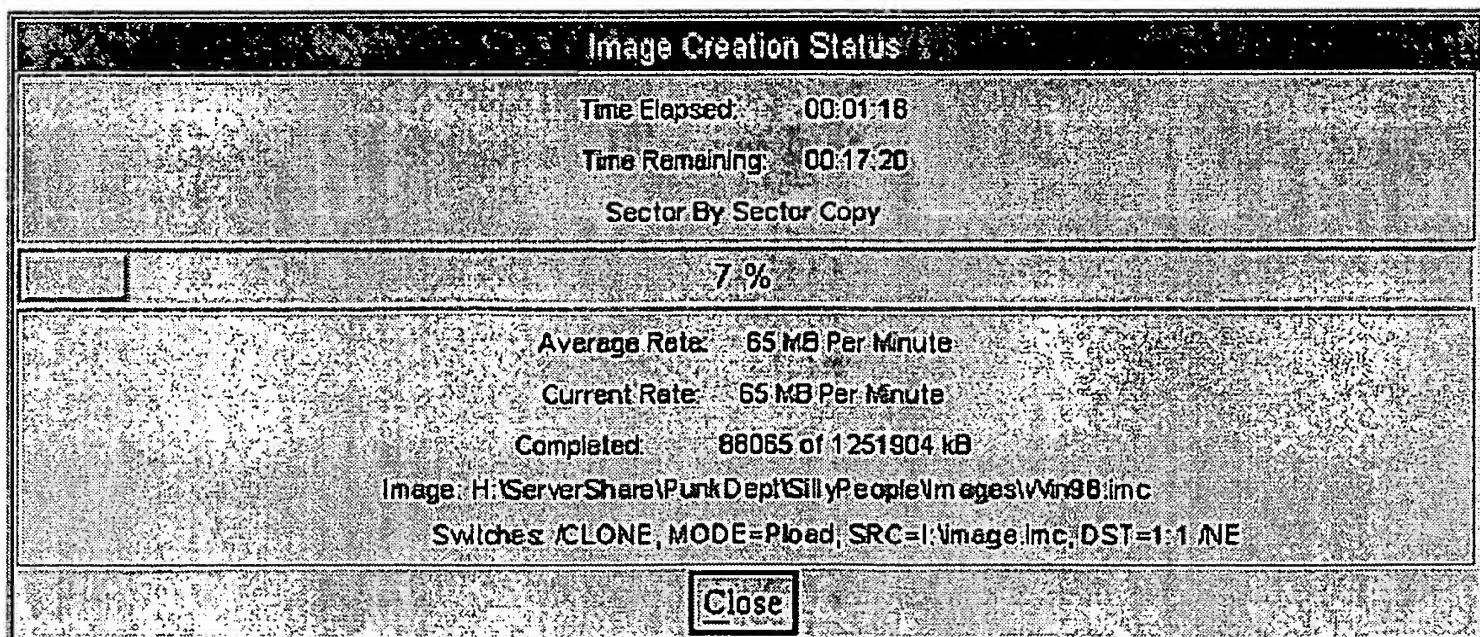


Figure 6 Client Image Creation screen

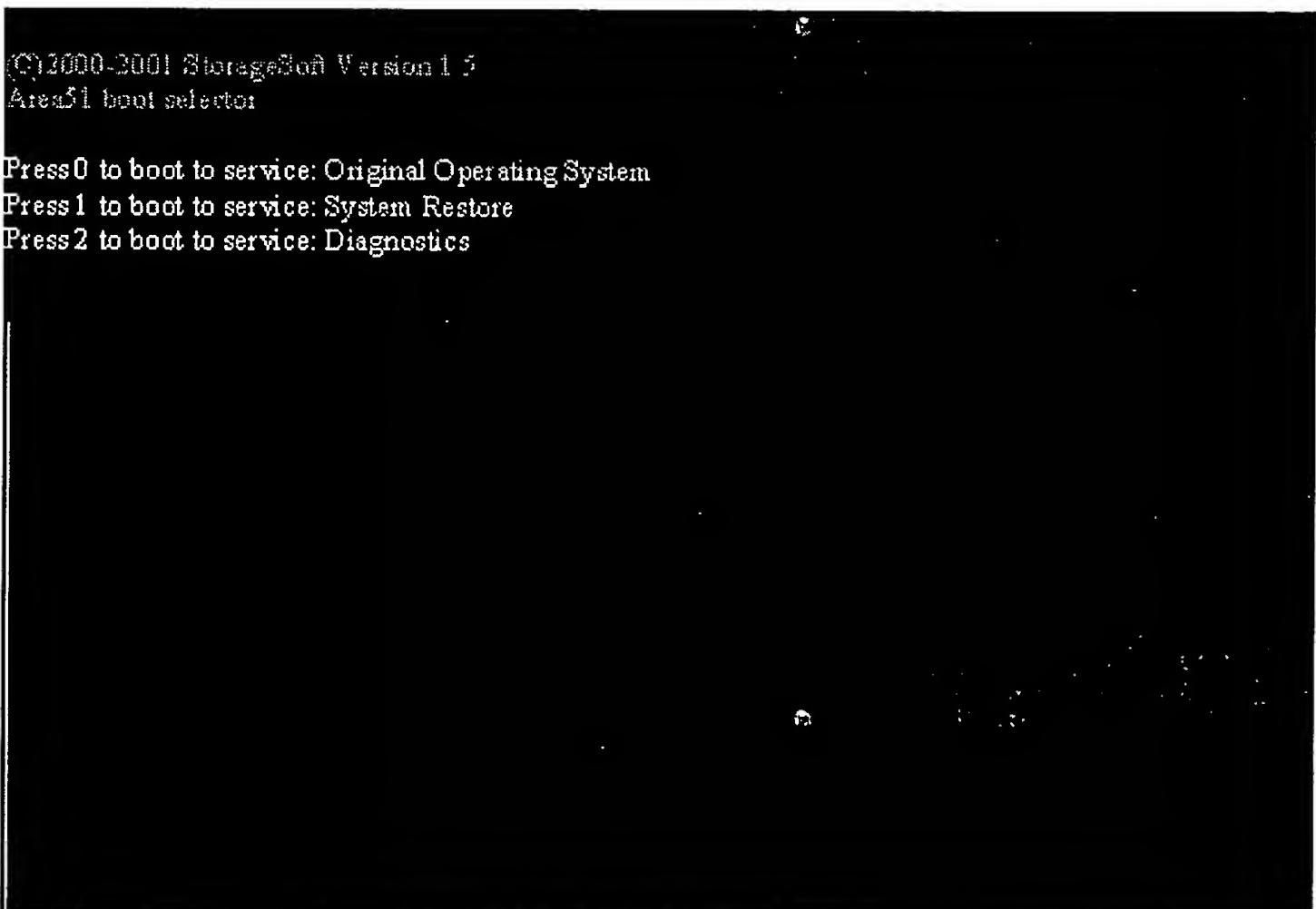
### 5.3 Using Area51 for imaging via PXE and disaster recovery

In this scenario, a PC is not only imaged with an operating system but also includes a Protected Area that stores the original manufacturer's configuration for the PC. This image can be used by the end user for disaster recovery and replaces the need for the manufacturer's restore CD. A second service can be installed in the Protected Area to provide diagnostic services to the end user in the case of an operating system failure.

To create this process, a boot image is created of an Area51 setup diskette that creates one service for disaster recovery or imaging and may also create additional services to store files for diagnostics or other purposes. Each service can have files copied to it via the script file from a mapped network drive, CD-Rom drive or any DOS drive letter.

For imaging the image file, ImageCast Client files and an appropriate autoexec.bat and config.sys file need to be copied into the recovery service. The easiest way to create the autoexec.bat and config.sys files is to use the ImageCast ClientBuilder or RestoreBuilder. Once these files have been copied into the service, the PXE server can facilitate boot into the Protected Area upon next reboot, and the image file is restored to the remainder of the hard drive. Currently, a hot key can be implemented using Area51 to allow boot into any of the services prior to booting to the OS. This hot key creates a Directory of Services that appears as a menu when the hot key is pressed so that users can select the service from which to boot or boot from the OS. The default boot is into the OS or User Area. The hot key is optional in cases where the Protected Area is supported by the BIOS.

The manufacturer's original image is restorable by simply pressing the hot key and selecting the appropriate menu item. Once the image is restored the first time, the PC is ready to be shipped to the customer with a disaster recovery solution on the hard drive. The following screen shot displays the menu that the hot key installs to allow the user to boot into system recovery, diagnostics or the original OS.



*Figure 7 Area51 Boot menu, displayed after hot key press*

## 6 Conclusion

The above scenarios describe a few of the options available when combining the powerful tools available from StorageSoft, Inc. The processes described would increase the efficiency of most PC manufacturing operations by eliminating many time-consuming steps and unnecessary human intervention.

The StorageSoft PXE Server allows Area51 and ImageCast MFG to run automatically upon boot of the PC to automate the manufacturing process. These examples illustrate a few ways to reduce the cost and improve efficiency in a PC manufacturing process.

In addition, there are numerous other implementations of these tools, together and separately, that can be modified to fit specific customer needs. Other features not discussed in this document include image layering, post configuration editing and automatic SID generation, to name a few. Utilizing these tools together or separately can renovate the way PCs are manufactured today.

## 7 Contact information

If you want more information about Area51 and ImageCast, please contact the StorageSoft Sales division at:

Phone: +1 (949) 415-0833

Email: [Sales@storagesoft.com](mailto:Sales@storagesoft.com)

StorageSoft web site: <http://www.storagesoft.com>



**StorageSoft**

StorageSoft.com

white paper

# Area51

*Onboard System Recovery*

Revision History.....	3
Disclaimer .....	3
<b>1 Abstract .....</b>	<b>3</b>
<b>2 Area51 Terminology.....</b>	<b>4</b>
<b>3 Area51 and Disaster Recovery.....</b>	<b>4</b>
<b>4 Area51 Benefits .....</b>	<b>5</b>
<b>5 Area51 Protected Area vs. Hidden Partition.....</b>	<b>5</b>
aka Host Protected Area vs. Hidden Partition Area .....	5
<b>6 Area51 Features.....</b>	<b>6</b>
6.1 Area51 Scripting .....	6
6.2 Accessing The Protected Area .....	6
<b>7 The Area51 Manufacturing Process .....</b>	<b>6</b>
7.1 First Process: .....	7
7.2 Second Process:.....	8
7.3 Third Process:.....	9
7.4 Fourth Process:.....	10
7.5 Fifth Process: .....	11
<b>8 Conclusion .....</b>	<b>11</b>

## Revision History

Date	Updated By	Changes
12/12/00	Jason Hayes	Initial Creation

## Disclaimer

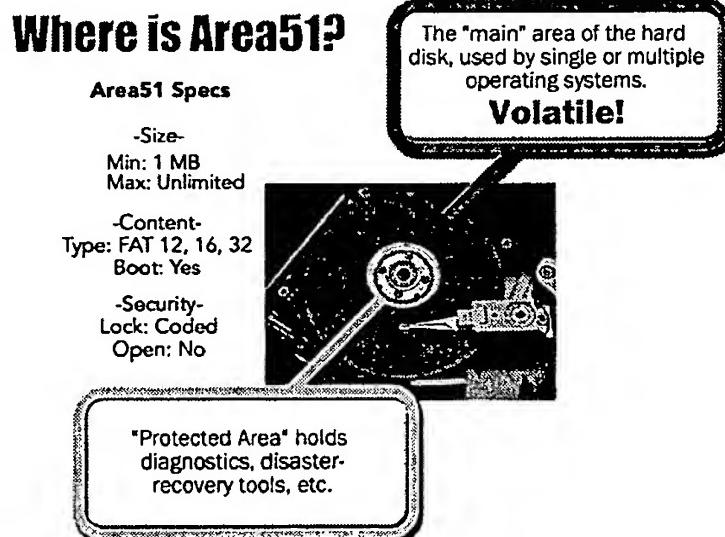
All "proprietary terms" defined in the course of this document are considered trademarks of StorageSoft Inc. and may not be used by any third parties without explicit indication of such ownership (e.g., by use of the "trademark symbol": ™ ).

The information presented in this document is to be considered the "best advice" our organization has to offer, however there is no warranty - implied or otherwise - that the given information will give predictable results under any conditions. By applying the information presented here, the reader is making an agreement to accept any and all responsibility of actions taken, based upon said information. The reader also agrees to hold StorageSoft Inc., as well as its agents, representatives, partners and affiliates harmless in the event that applying said information results in manifest damages of a real or conceptual nature.

Some of the concepts and methods described in this document may be covered under U.S. Patent.

## 1 Abstract

In 1998 the T13<sup>1</sup> Technical Committee outlined in the ATA<sup>2</sup> specification whereby an area of a hard drive could be reserved and protected from the normal end-user data area. This specification, known as the Protected Area Run Time Interface Extension Services (P.A.R.T.I.E.S.), allows OEM hard drive and PC manufacturers to store utilities, applications, and other data in the protected area without the worry of virus or user data integrity compromise.



**Eliminate foreign attacks to the hard drive!**

Figure 1 The figure above conceptually illustrates a hard drive platter with a Protected Area.

<sup>1</sup> T13 is a Technical Committee of Accredited Standards Committee NCITS.

<sup>2</sup> AT Attachment with Packet Interface - 5 (ATA/ATAPI-5)

With today's large hard drive capacities, the effect of reserving a portion of the total capacity on the drive for a protected area is negligible. Even with the existence of a protected area, end users still have a vast amount of space on the drive with which to save data. In fact, this protected area is so well hidden that users most likely won't know about its existence unless specifically informed.

## 2 Area51 Terminology

To absorb and apply the knowledge presented here, it is helpful to have a basic understanding of the terminology surrounding Area51:

**Logical Block Address (LBA)** A method of addressing the sectors on a hard drive in a linear format. Hard drives generally contain millions of sectors, these sectors are where the data is stored on the drive. LBA simply maps each sector out in a linear manner, the first sector on the drive is LBA 0, the second sector is LBA 1, etc.

**SETMAX Address** The ATA command that, when sent to the drive, sets the last addressable sector in the user area. Generally, this command is used to reduce the total capacity of a hard drive when first initiated in order to create the Protected Area.

*Cm2* **Protected Area** The reserved and protected space on the hard drive not normally accessible to the user. While booted to the Operating System the Protected Area is completely hidden and inaccessible.

*Cm2* **Service Area** A sub-area within the protected area where files can be stored. Service areas allow files to be organized and grouped together by program type, i.e. all diagnostic programs can be stored in the same service area, and disaster recovery programs can be stored in a separate service area.

*Cm1* **User Area** The area of the hard disk that is available to users. The user area is where the Operating System, Application programs, and user-stored files reside.

*Cm1* { **BIOS Engineering Extension Record (B.E.E.R.)** A data structure located in the last sector of the drive that contains information about the Protected Area and Directory of Services. The ATA SETMAX Address command hides this structure.

**Directory of Service (DoS)** A BIOS readable string contained in the BEER that allows the BIOS to present a meaningful name for each serviceable area available to the user once the Protected Area is accessed.

## 3 Area51 and Disaster Recovery

In response to the new specification outlined above, StorageSoft Inc. has developed a suite of utilities known as *StorageSoft Area51™*, that combines StorageSoft's current hard drive imaging technology and protected area technology to provide disaster recovery. These utilities allow a backup image of a hard drive to be stored, and restored, from the Protected Area. *Area51* has a host of other options other than just storing image files, it can be used to create the Protected Area to store diagnostic files, backup files, or any other data deemed pertinent by a manufacturer.

The idea behind *Area51* is still relatively new in the industry and is just now beginning to garner attention with its possibilities. Both PC and hard drive manufacturers are now beginning to realize the potential of *Area51*.

Many PC manufacturers currently provide image files, or other such disaster recovery backups, of each system that goes out the door on a CD. Image files generally contain the Operating System and applications that are loaded at the factory before shipment to the customer. If the system becomes unstable out in the field, the image file can be restored from the CD and the system reset to its initial factory state. Shipping a CD with every system can be a costly venture. With *Area51* the image file can be stored in the protected area and then, if necessary, the image can be restored to the usable area of the hard drive thus restoring the system back to the initial factory state as shipped. Other manufacturers view *Area51* as a solution to troubling Non-Defective Failure (NDF) issues that have plagued the industry over the past few years.

When customers call technical support, it can be difficult for the technician to determine if the problem is an actual hardware defect or user error. Accurately determining the source of the problem can require a great deal of time per call, which is not cost effective. To combat this issue diagnostic programs have been written to determine if there is truly a defect or not, the problem has been how to get these diagnostics into the users hands. Either the manufacturer must provide diagnostics on a diskette to ship with every drive, which is very costly, or the software has to be downloaded from the Internet. Downloading from the Internet assumes the user has a working system, which is not always a feasible assumption to make. *Area51* solves these problems by allowing manufacturers to place critical diagnostic utilities at the users fingertips without adding the use of a diskette or downloading from the Internet.

These are a few basic application examples of the flexibility of *Area51*, a technology designed to be flexible to meet the complex needs of both manufacturer and user.

#### 4 Area51 Benefits

- Allows space on the hard drive to be reserved for manufacturer or system specific usage
- Puts diagnostic utilities and restore image capability at the end-users fingertips because these files are in the protected area as opposed to a diskette or CD.
- Eliminates the possibility of diagnostic or image media (diskette/CD) of being lost by the end user.
- Reduces product delivery and manufacturing costs by eliminating the need to ship a diagnostic diskette or restore image CD with the product.

#### 5 Area51 Protected Area vs. Hidden Partition

##### aka Host Protected Area vs. Hidden Partition Area

Many software utility packages utilize a hidden partition, or hidden partition area, to store diagnostic and/or disaster recovery applications. Because of the technology behind the product, many people confuse the *Area51* Protected Area with a hidden partition, however there is an important distinction between the two. Although the hidden partition is not readily accessible in the operating system environment, there is still record of its existence in the partition table. Using a partition utility such as FDISK or other partitioning applications will identify this partition as Non-DOS, which is why Microsoft operating systems don't assign it a drive letter. Since the partition table does contain a record of the hidden partition, it is susceptible to virus attacks and possible corruption from user error via hard drive utilities such as Partition Magic, the aforementioned FDISK, and various Norton Utilities applications.

Unlike hidden partitions, there is no record of the *Area51* Protected Area/Host Protected Area in any of the normal hard drive records, ie the partition table, file allocation tables, and DOS boot record. Essentially the area does not exist, the operating system won't see it, virus' won't see it, and the user may not be aware of its existence unless specifically informed. The data contained in the *Area51* Protected Area is truly hidden and secure.

## 6 Area51 Features

StorageSoft Area51 utilizes custom command line switches to create the Protected Area on a hard drive. All of the switches for creating a Protected Area can be entered into a text file, Area51.exe can then reference the text file for instructions on how to create the area.

### 6.1 Area51 Scripting

The benefit of using a script file to create a protected area is automation, which is key in a manufacturing and enterprise environment. Utilizing a script file allows the protected area to be created, populated with data, and protected automatically, eliminating the need for technician input, which boosts the productivity of the manufacturing or configuration line.

Scripting is a feature that is usually program specific, meaning the definition of scripts, the syntax used to create scripts, and the functions of scripts is defined by the program developer. This can cause confusion for the user who may not be familiar with the program or the technology behind the program. To help educate users with Area51 scripting StorageSoft has developed a Windows based tutorial that assists users with creating a successful script file.

### 6.2 Accessing The Protected Area

There are varieties of ways the Protected Area can be accessed once it has been installed onto the hard drive. Since this area is truly protected from the Operating System, accessibility to the PA must occur during a system boot. The methods for accessing the PA are as follows:

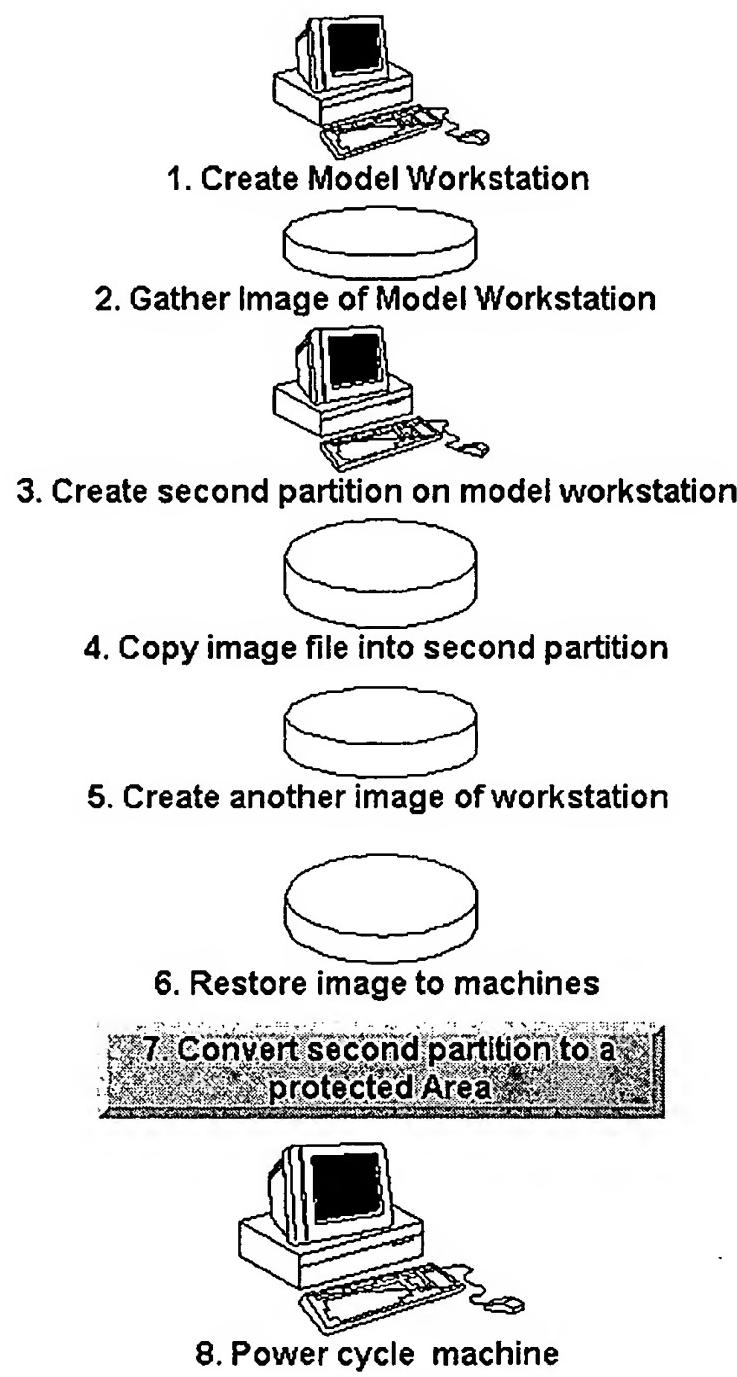
1. **System BIOS-** BIOS manufacturers such as AMI and Phoenix are in the process of implementing protected area support into their BIOS EPROM's. During the Power On Self Test (P.O.S.T.) portion of the boot the BIOS will likely provide a hot key, if the button is pressed the system will boot directly into the Protected Area instead of the Operating System.
2. **Master Boot Record (MBR) code-** StorageSoft currently has the technology to place a custom Master Boot Record onto the hard drive. When the system boots from the hard drive the MBR code will execute and, similar to the BIOS solution above, will allow users to press a hot key to boot into the Protected Area. This is an ideal solution for legacy systems that do not have a BIOS that supports the Protected Area.
3. **Recovery diskette-** This method will allow users to access the Protected Area by booting from a diskette. This method is also an ideal solution for legacy systems but has the disadvantage of requiring a boot floppy to be shipped with the system or hard drive.

## 7 The Area51 Manufacturing Process

Not all PC manufacturing processes are the same, for example the methods Gateway uses to assemble and load data onto a system on the manufacturing line could be vastly different or slightly different from Dell's methods. To account for different PC manufacturing methodologies StorageSoft has developed a series of Area51 implementation processes based on prevalent manufacturing procedures. The Area51 implementation processes are outlined in the following pages. The flowcharts illustrate how StorageSoft's *Area51* creates the Protected Area, stores files in the Protected Area, and allows image files to be restored from the Protected Area.

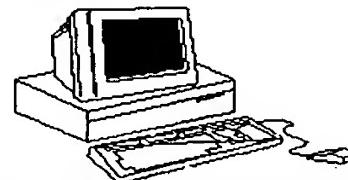
### 7.1 First Process:

A common scenario for a manufacturer will be to gather an image, then to setup Area51 on a drive that is to serve as model workstation for the rest of the manufacturing process. One way in which to accomplish this task is to setup the drive as the end user will see it, but also create a partition that will become a protected area, which the end user cannot access.

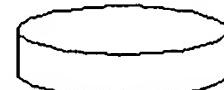


## 7.2 Second Process:

The second method is to create a model workstation, then distribute the image using only a portion of the space on a target hard drive. With the excess space, Area51 can create a protected partition.



**1. Install operating system and other applications  
on model workstation**



**2. Gather image of model workstation**



**3. Distribute image to machines, using a portion of the space on the drive**

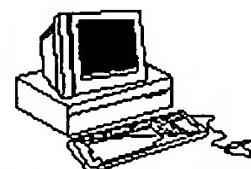
**4. With scripting, use the Area51 program to create a protected  
area, copy the image and other files into the protected area, lock  
down the partition.**



**5. Power cycle machine**

### 7.3 Third Process:

Another common scenario will be to gather an image that has two partitions, then to convert the second partition to a protected area.



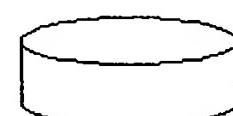
1. Create Model Workstation with two partitions



2. Gather Image of Model Workstation

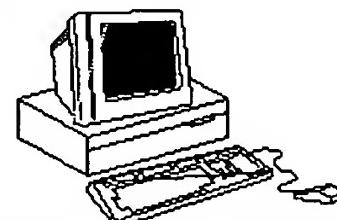


3. Distribute image to machines



4. Copy image and client files into second partition

5. Convert second partition to a  
protected Area

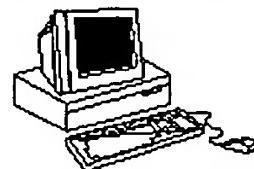


6. Power cycle machine

#### 7.4 Fourth Process:

There may be situations in which it would be advantageous to create a protected area first, then setup a model machine and then gather the image into the protected area. This situation may be best suited for an assembly line that is preparing machines with different files and/or operating systems, but will all have a protected area.

##### 1. Create an Area51 partition on machines



##### 2. Install operating system and application on model machines

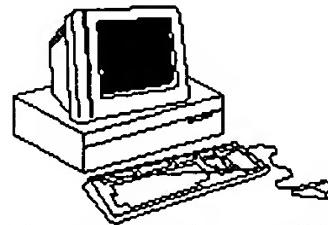


##### 3. Gather image of model machine



##### 4. Distribute image to machines

##### 5. Unlock the protected area, copy image and other files into protected area, lock down the partition via scripting.



##### 6. Power cycle machine

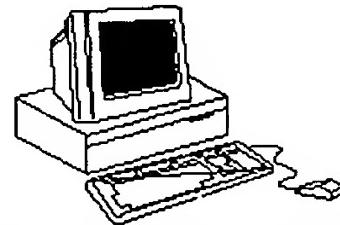
### 7.5 Fifth Process:

Current users of ImageCast will have a library of images that they will wish to deploy, but will also want to use with Area51. The client has the ability to restore an image to only use a certain amount of space on a drive. With the extra space left on the drive, Area51 can create a protected partition.



1. Distribute image to machines, using a portion of the space on the drive

2. With scripting, use the Area51 program to create a protected area, copy the image and other files into the protected area, lock down the partition.



3. Power cycle machine

## 8 Conclusion

As PC technology continues to grow, the need to provide end users with comprehensive utilities and files to manage and troubleshoot this technology will continue to be a requirement. Area51 is a flexible technology that both PC manufacturers and enterprise companies are embracing to address this requirement, while simultaneously adding the benefit of reduced product delivery costs. With Area51, shipping costly supplemental CD's and floppy diskettes with OEM products will go by the wayside because the data contained on this media can now be stored in the Protected Area. Area51 provides convenience to the end-user because they will no longer need to keep track of multiple CD's or diskettes since these programs and files will already reside on their hard drive. Though still an infant technology, Area51 figures to play a prominent role in the PC industry to provide a myriad of solutions as the PC industry continues to evolve. Because of its flexibility, Area51 will be in position to handle the PC evolution to provide these solutions quickly and cost-effectively.

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
  - IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
  - FADED TEXT OR DRAWING**
  - BLURRED OR ILLEGIBLE TEXT OR DRAWING**
  - SKEWED/SLANTED IMAGES**
  - COLOR OR BLACK AND WHITE PHOTOGRAPHS**
  - GRAY SCALE DOCUMENTS**
  - LINES OR MARKS ON ORIGINAL DOCUMENT**
  - REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
  - OTHER:** \_\_\_\_\_
- 

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**